DEFENSESTORM
THE BEST OFFENSE.

BRAND GUIDE

Last updated August 2023

OVERVIEW

As DefenseStorm's brand messaging evolves, so do our brand guidelines. We developed our new brand mark, color palette, typography and imagery to reflect the message of DefenseStorm as the best offense. This tagline highlights our platform's 360-degree approach to proactively identifying and neutralizing cyberthreats before they gain a foothold in our clients' networks. All our brand elements work together to position DefenseStorm as an ally, ready to help our clients take charge of their cybersecurity.

This guide offers an in-depth exploration of each brand element, along with do's and don'ts for leveraging the brand in sales and marketing materials. It concludes with several asset examples using the new branding.

Questions on proper brand usage?

Reach out to marketing before proceeding. Contact Mia Callicutt at mia.callicutt@defensestorm.com.

LOGO & MARK

LOGO

Primary Logo

DEFENSESTORM

Tagline Logo

DEFENSESTORM
THE BEST OFFENSE.

Brand Mark

DS

Our logo is a visual representation of the new DefenseStorm brand.

We have three different depictions of the logo:

Primary: The primary logo should be used in internal communications, communications with existing clients (e.g. quarterly business review decks), and co-branded sales materials (e.g. case studies).

Tagline: The tagline logo should be used in any non co-branded sales materials that might be considered "first touch" (e.g. sales sheets that live on the website, decks for prospective customers, tradeshow signage). It should also be used on any materials that include our brand boilerplate (e.g. press releases). It is designed as a conversation starter.

Brand Mark: In instances where the primary or tagline logo are not usable, such as the website favicon, the brand mark can be used as an alternative.

DEFENSESTORM
THE BEST OFFENSE.

DEFENSESTORM
THE BEST OFFENSE.

CLEAR SPACE

To maintain the integrity of our brand and logo, it's important to allow the logo breathing room. The minimum amount of space between the DefenseStorm logo and another object should be the width of the 'D' in the logo.

Cobranding

DEFENSESTORM + LOGO

Cobranding:

DefenseStorm works closely with financial institutions to protect their data. Sometimes it will be necessary to show our logo next to our clients' logos. This is how we do it.

We should always adhere to clear space guidelines. For separation, we like to use a plus sign. This signifies a collaborative and mutually beneficial relationship.

WHAT NOT TO DO

DEFENSESTORM

A Do not add drop shadow or other effects to the logo.

DEFENSESTORM

C Do not stretch or squish the logo.

DEFENSESTORM
The Best Offense.

E Do not manually add the tagline or strapline to the logo.

G Do not place the logo on a background that makes it hard to see.

DEFENSESTORM

B Do not color logo outside of regulated color options.

DefenseStorm

D Do not change proportions of the logo elements.

DEFENSESTORM

F Do not change the fonts of the logo.

DEFENSESTORM

H Do not rotate the logo.

To create a strong and consistent brand, our most representative element must always be treated properly. Our logo should never be tampered with including but not limited to the ways listed below.

A Do not add drop shadow or other effects to the logo.

B Do not color logo outside of regulated color options.

C Do not stretch or squish the logo.

D Do not change proportions of the logo elements.

E Do not manually add the tagline or strapline to the logo.

F Do not change the fonts of the logo.

G Do not place the logo on a background that makes it hard to see.

H Do not rotate the logo.

COLOR PALETTE

COLORS

YELLOW

C1 M31 Y100 K0
R249 G182 B23
HEX #F9B617

RED

C0 M89 Y99 K0
R239 G68 B35
HEX #EF4423

GRADIENTS

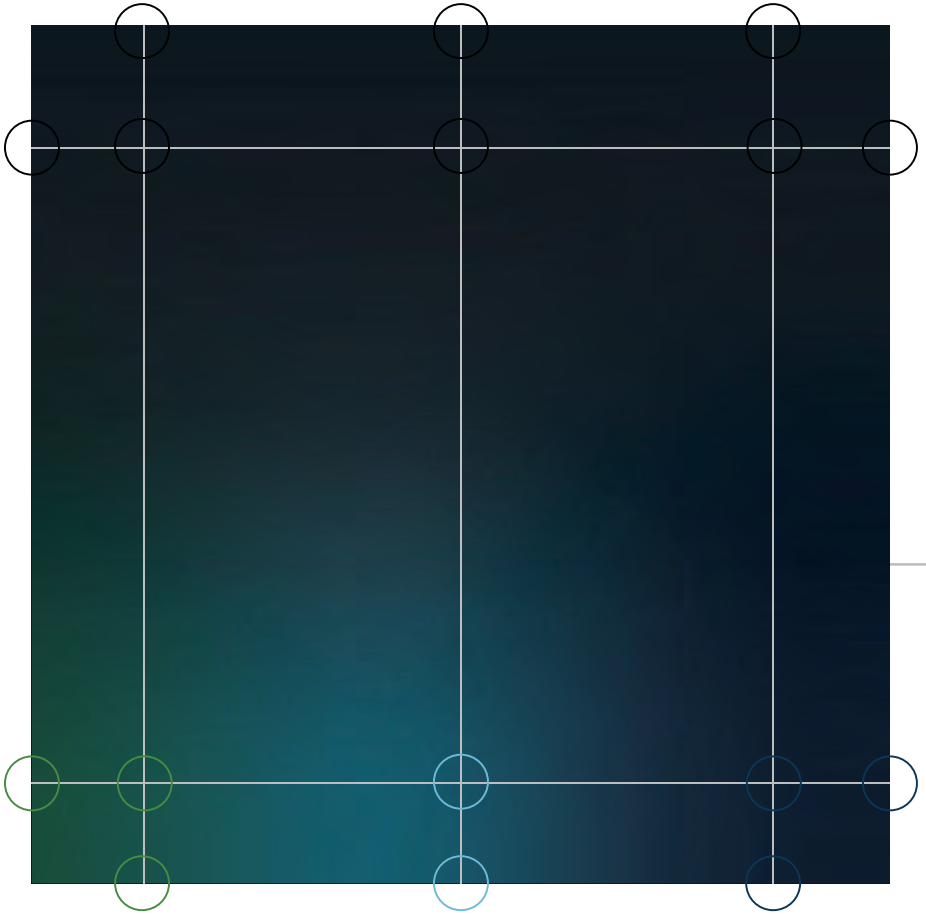
In lieu of an extended color palette, colors can be combined into gradients to add dimension to the DefenseStorm brand.

Gradients can be applied in a linear approach in or as a mesh gradient with multiple colors and opacities.

The blue and green gradients pictured here are linear gradients.

GRADIENTS

BLACK
HEX #000000
Opacity: 0%



BACKGROUND
NAVY
HEX #0C171E

GREEN
HEX #468C41
Opacity: 100%

SKY BLUE
HEX #6EBBD9
Opacity: 100%

DARK BLUE
HEX #0B3656
Opacity: 100%

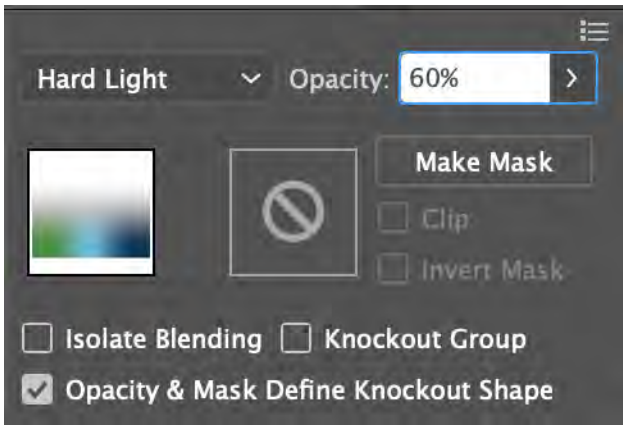
To create the multi-color gradient, create a gradient mesh with points in the denoted locations.

The points on one side of the mesh should all be black at 0% opacity.

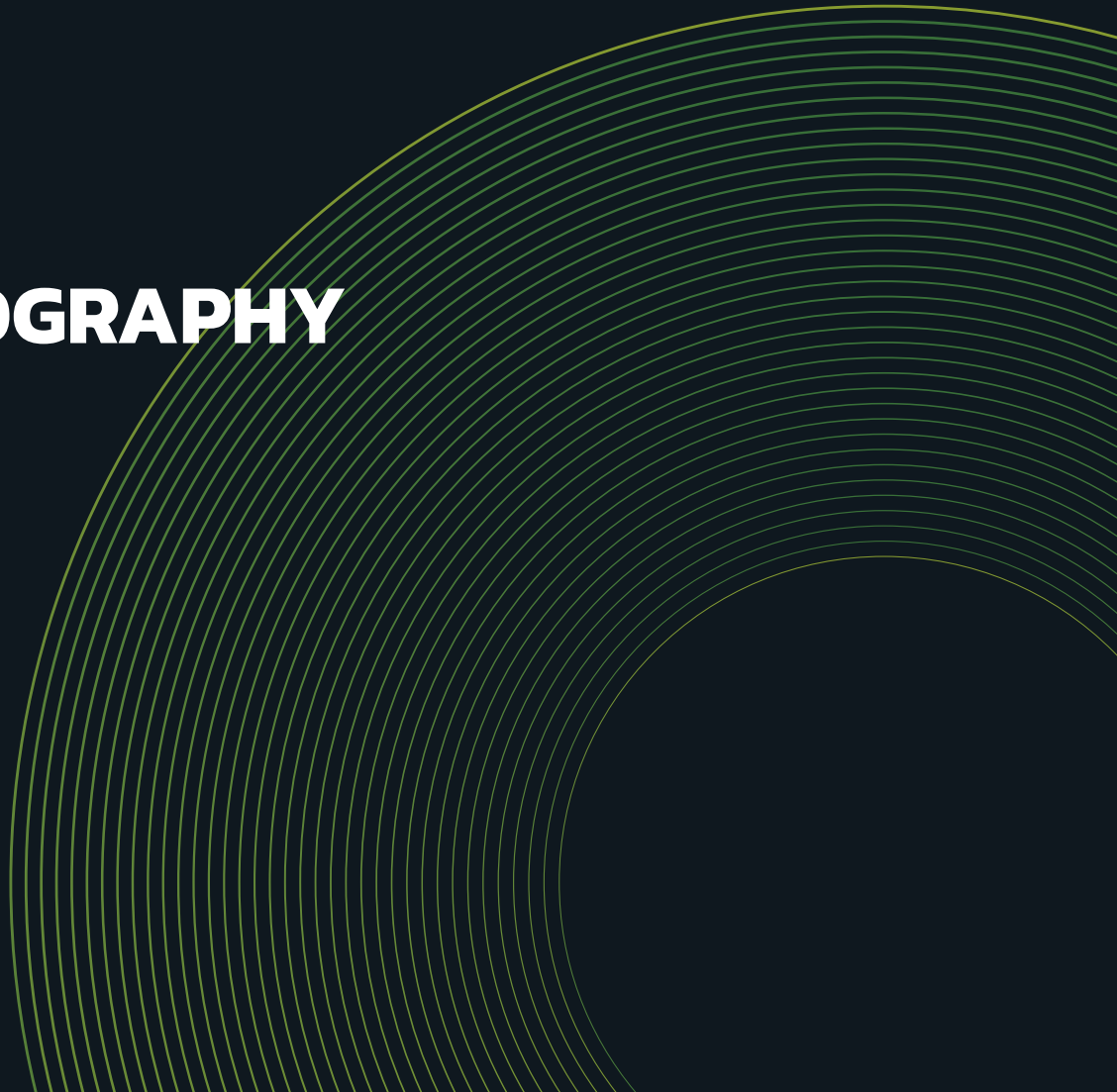
The points at the other side should be green, sky blue, then dark blue, all at 100% opacity.

Place the gradient mesh on top of a shape of the same size in navy.

Make the full gradient mesh 60% opacity, and turn on the Hard Light blending mode. Then check the box for 'Opacity & Mask Define Knockout Shape'.



TYPOGRAPHY



TYPOGRAPHY

Primary
Header Typeface

Aa

KANIT

Thin ExtraLight Light **Regular**
Medium SemiBold Bold
ExtraBold Black

Primary
Body Typeface

Aa

LATO

Light **Regular** Medium
Semibold **Bold** Heavy **Black**

System
Typeface

Aa

CALIBRI

Light Regular **Bold**

TYPOGRAPHY STYLING

H1 IS SET IN KANIT BOLD IN WHITE OR NAVY

h2 are set in Lato Heavy in dark blue

Body copy is set in Lato Light in black.

We recognize the unique risk factors that FIs face so they can address their cyber risk with a unique solution. That's why we set out to build a cyber risk solution that is unique for banking.

h3 are set in Lato Bold in black

- bullets are also set in Lato Light in black
- bullets are also set in Lato Light in black
- bullets are also set in Lato Light in black

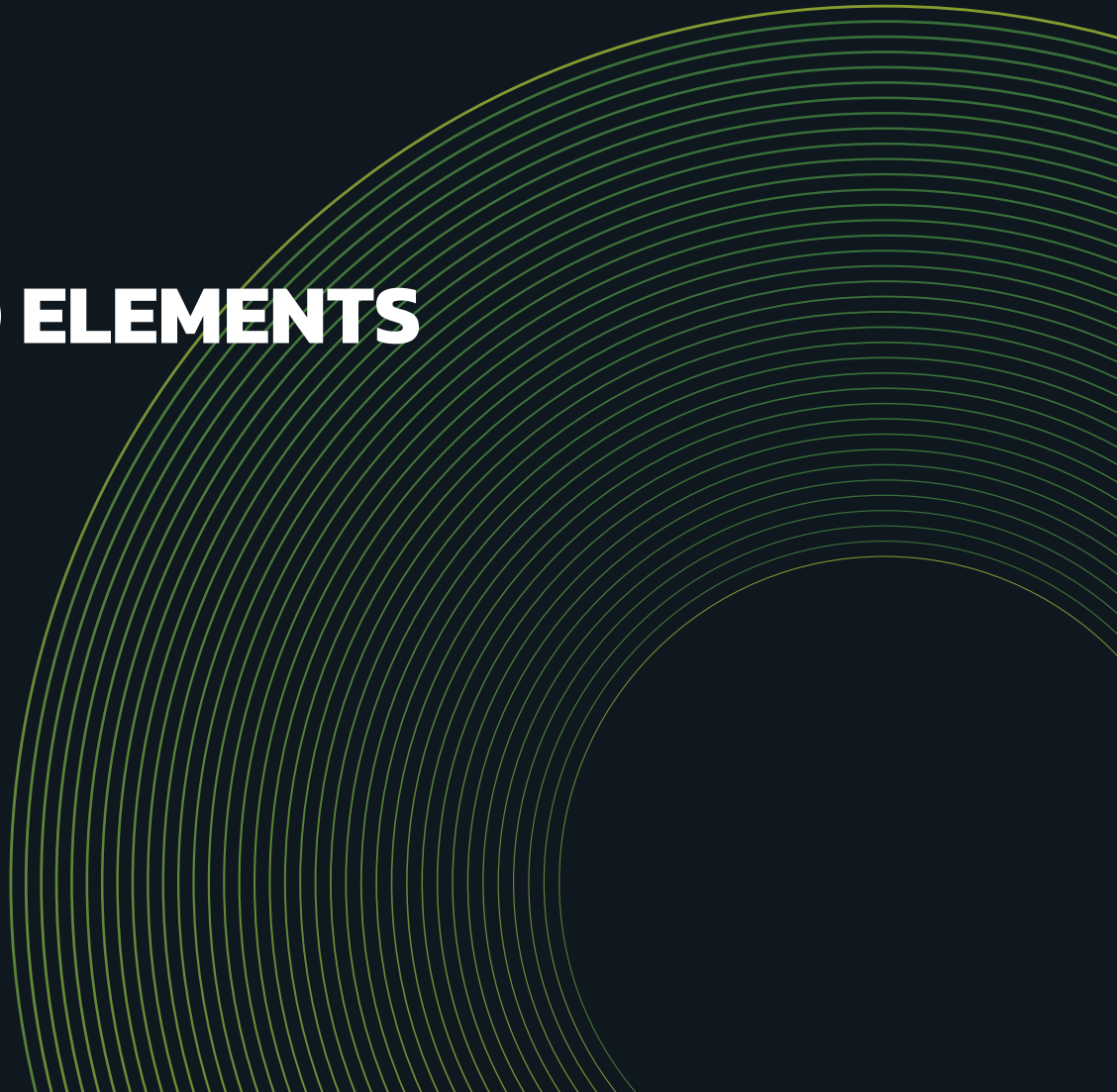
Kanit and Lato should be the only two fonts used in our brand any time they are available. Kanit should be used for headlines, while Lato should be used for subheadlines and body.

Headlines should be set in a combination of Bold & Light to create emphasis and mimic the DefenseStorm logo styling.

Leading for headlines using Kanit or Lato should be about 85% of the typeface point size. This keeps text tight, but still with room to breathe. Set the kerning to -10.

Body copy should be set in 10pt font, 0 kerning, with 12pt leading, or leading 120% larger than the font size.

BRAND ELEMENTS



GRADIENT RING

There are two styles of the gradient ring used in the DefenseStorm brand. The first is one large, solid ring. The second is concentric thin rings, creating a large partial circle full of visual texture.

The gradient ring can also be blue, going from sky blue to dark blue.

GRADIENT RING USAGE

The gradient ring can be used in a few ways. In large images with a defined subject, the ring can be used as a background element, tucked behind the subject of a photo.

In smaller photos placed in a circular frame, the ring can be an overlapping element.

When cropping photos into a circle, ensure that the subject is in the frame. Do not crop out bodies/heads and leave only hands visible.

GRADIENT RING USAGE

The first step is to understand the following:

- Security Operations Center (internal vs. external)
- Three management approaches
- Types of IT security
- Tools vs. technology and services

What is an internal SOC vs. an outsourced SOC?

A Security Operations Center (SOC) is a department that focuses on the safety and security of daily cyber operations. Internal teams are created to identify potential threats and mitigate breaches. Many financial institutions don't have an actual team or department; they only employ a few personnel to review logs.

An outsourced SOC or a Security Operations Center as a Service (SOCaaS) is an external cyber risk management company hired to either co-manage the monitoring process with an organization's existing SOC or fully manage and maintain their cyber risk management needs.

What are the benefits of outsourcing a SOC?

Organizations that operate with only an internal SOC are inundated by the demands of detection and mitigation of cyberattacks. It is practically impossible for businesses to retain enough manpower for 24/7/365 monitoring because the cost to employ the necessary number of personnel surpasses their financial capability.

When teams are overwhelmed by the volume of data and events to scrutinize, mistakes happen, and breaches occur. This is true for FIs who employ a whole team but even more so for those functioning with only 1 or 2 people tasked with reviewing logs. An outsourced SOC is the first line of defense to identify suspicious activity or a possible breach. The threats are then evaluated and escalated to the internal team or managed by a full-service SOC.

DEFENSESTORM
THE BEST OFFENSE

How to Remain Secure in the Cloud and Adhere to the New FFIEC Guidance

Financial institutions are making changes to how they support internal users, infrastructure and account holders in response to the COVID-19 global pandemic and the rapidly evolving digital landscape. With the transition to a remote workforce, many have been leveraging cloud-based services to safeguard customer information and maintain compliance.

To address the proper use of these cloud computing services, the Federal Financial Institutions Examination Council (FFIEC) recently issued a statement that included a risks associated with outsourced cloud-based services.

Because DefenseStorm is a cloud-based cybersecurity provider, we have outlined some mitigate risks.

Addressing Relevant Risk Management Practices

The FFIEC statement focuses primarily on steps institutions should take to address cloud computing outsourcing of common service models including:

- Software as a Service (SaaS): Utilizes internet to provide applications, which are managed by the vendor. These services include Salesforce.
- Platform as a Service (PaaS): Delivers frameworks for developers that can be used to create customized applications. These services include Force.com, Azure and AWS.
- Infrastructure as a Service (IaaS): Encompasses a full self-service cloud infrastructure for accessing and monitoring computers. These services include AWS and Windows Azure.

The guidelines state that a financial institution cannot assume operating in the cloud inherently ensures the appropriate security controls and oversight are in place, and that leveraging the computing environment is critical to ensuring safety and soundness.

At DefenseStorm, we diligently follow and implement FFIEC guidelines to ensure we are doing what is best for our customers. Our cybersecurity and cybercompliance technology was designed as a adhere to FFIEC guidance, regardless of which cloud-based service model is deployed, detect and prevent fraud before money goes out the door.

DefenseStorm and the New FFIEC Guidance

DefenseStorm has been working with financial institutions that have implemented cloud services for years, allowing us to build a core competency in satisfying the kind of guidance the FFIEC released. For those institutions that are interested in future deployment and security risk management principles, we can leverage that experience to ensure compliance. Our all-in-one solution unites cybersecurity detection, investigation and reporting with compliance; all in real time.

Built specifically to accommodate the evolving financial systems of today and tomorrow, we aim to be a real partner to banks and credit unions that want to follow FFIEC guidance on security in a cloud computing environment by:

- Working with customers to align strategy, architecture, compliance and risk goals that suit
- Helping to monitor and mitigate risks with a co-managed platform that delivers cyber safety and soundness.
- Consolidating security data so customers can oversee entire security operations in real time
- Connecting policy and regulations with cyber controls that have built in frameworks (FFIEC CAT/ACET) to maintain compliance standards;
- Making reporting and proving compliance easy.

DEFENSESTORM

Real Time Cyber Safety and Soundness

Cloud-based service solutions aren't going anywhere. If anything, they are growing more prevalent. While remote work might have accelerated the adoption of cloud computing, it will soon be a well-established system.

The concentric thin line gradient rings are typically used as a background element, seen on the divider pages of this brand guide, and also shown here in two examples of a data sheet and an interior page of the Buyer's Guide.

In addition to the concentric thin line rings, this page from the Buyer's Guide also features the solid ring in use in the header image, and a gradient and is a good example of how brand elements work together.

PHOTOGRAPHY

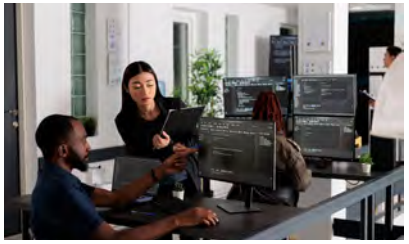
PHOTOGRAPHY









The imagery in our brand is meant to be intriguing to the audience, while the use of people brings warmth and authenticity. To reflect our brand, the photos often feature a dark background or dark hardware with a tech-office feel. The subjects should not be looking directly at the camera, but instead interacting with their environment. The subject should not look worried or afraid, but instead show confident people who are exceling with trust in their cyber security provider. Bonus points if the subject is wearing a brand color.

ICONOGRAPHY

ICONOGRAPHY

Isometric illustrations are used to show DefenseStorm's processes. Here are a few of the illustrations created for the website, marketing materials, and other use cases.

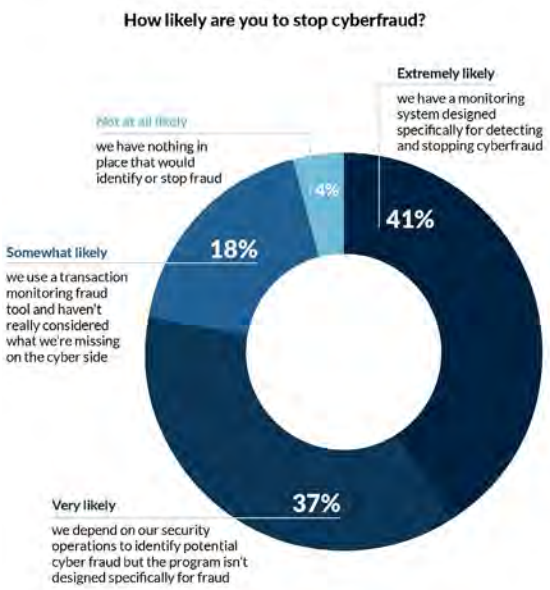
Illustrations are created in a primarily light grey neutral pallet with pops of brand colors to pull focus to elements of the illustrations

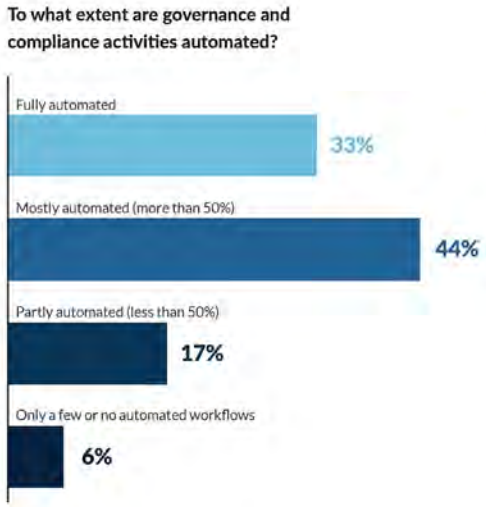
ICON USAGE

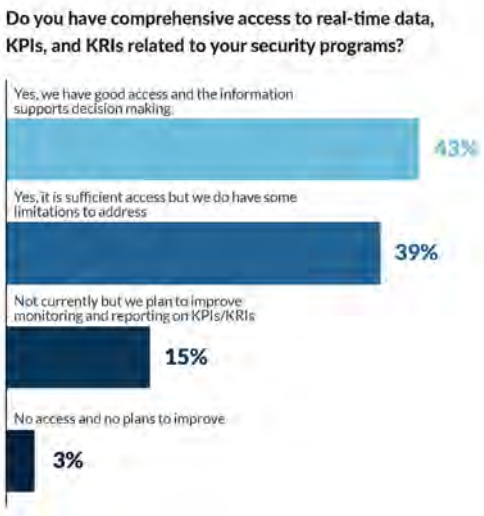
Here are a few of the use cases for the isometric illustration icons.

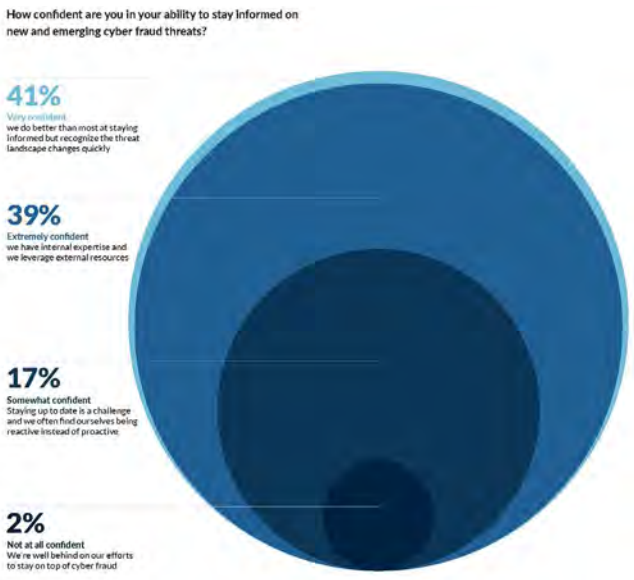
DATA VISUALIZATION

DATA VISUALIZATION







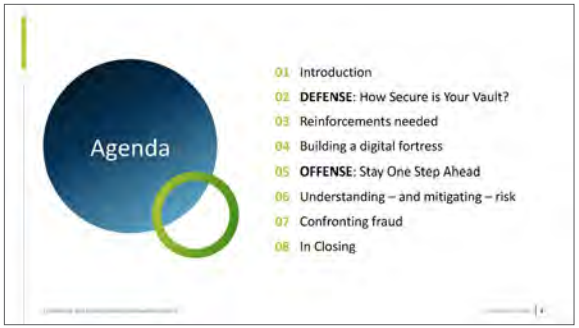


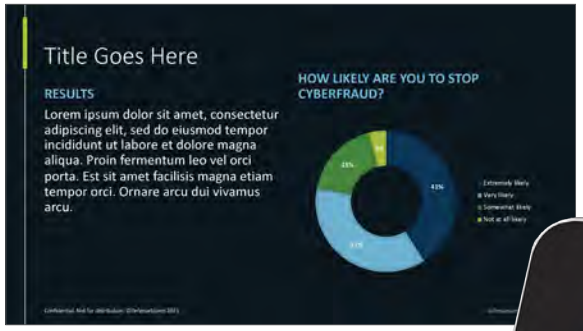
When creating charts, follow a consistent color pattern. The charts should utilize the brand blues, going from lightest to darkest or darkest to lightest, in color order. If additional colors are needed, white, black and the DefenseStorm green, lime & yellow can be used as well.

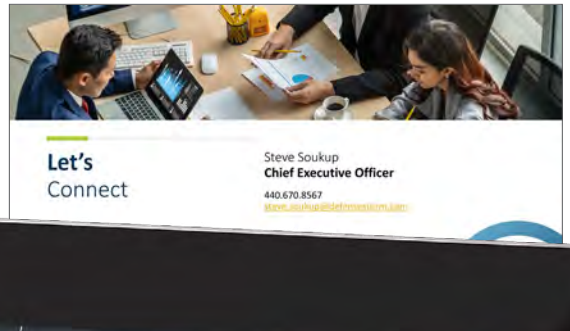
ASSET EXAMPLES

BUSINESS CARDS

POWERPOINT


Agenda
01 Introduction
02 DEFENSE: How Secure is Your Vault?
03 Reinforcements needed
04 Building a digital fortress
05 OFFENSE: Stay One Step Ahead
06 Understanding – and mitigating – risk
07 Confronting fraud
08 In Closing

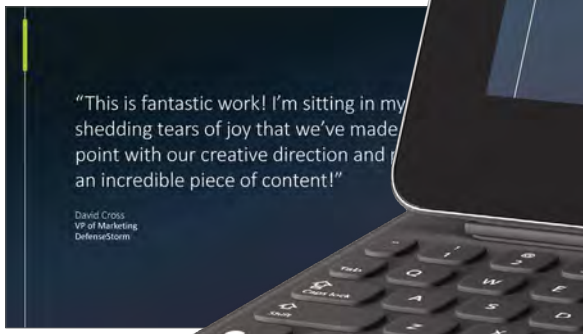

Title Goes Here
RESULTS
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Proin fermentum leo vel orci porta. Est sit amet facilisis magna etiam tempor orci. Ornare arcu dui vivamus arcu.
HOW LIKELY ARE YOU TO STOP CYBERFRAUD?


Let's
Connect
Steve Soukup
Chief Executive Officer
440.670.8567


DEFENSESTORM
Click to add section title
This is a new section


STEVE SOUKUP


Title Goes Here
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Proin fermentum leo vel orci porta. Est sit amet facilisis magna etiam tempor orci.
Ornare arcu dui vivamus arcu.
In arcu cursus euismod quis viverra.
Velit sed ullamcorper morbi tincidunt ornare.
In fermentum posuere urna nec.


David Cross
VP of Marketing
DefenseStorm

DEFENSESTORM
THE BEST OFFENSE
Presentation Title Goes Here
This is a brief introduction to the presentation

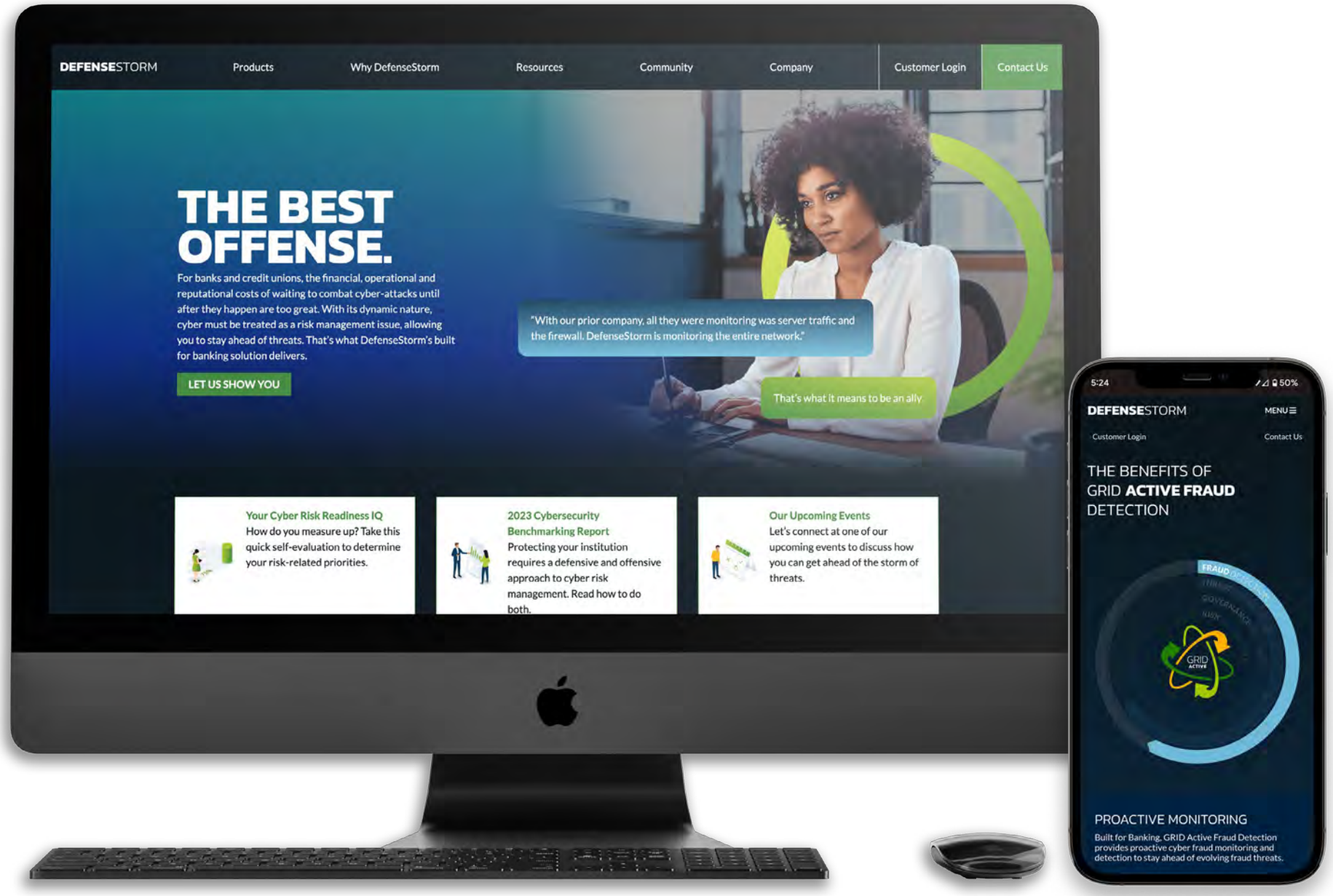
ONE PAGERS


DefenseStorm Governance Program
DefenseStorm Governance Program
Governance and Monitoring
Integrated Frameworks
DEFENSESTORM +
BMTX AND DEFENSESTORM UNITE TO STOP CYBERFRAUD
The Challenge
The Solution

WHITE PAPER


2023 Cyber Risk Benchmarking Report:
How Financial Institutions Play Defense and Offense
Financial institutions (FIs) operate in an environment of constant change, and therefore constant risk. Expanded digital offerings, upgraded technology at existing branches or opening new branches are all reasons to celebrate change, but if FIs aren't careful, these advancements open the door open to even more risk. Cyber criminals are always on the watch, seeking out weaknesses that enable them to penetrate your defenses. Banks and credit unions need to measure the implications that changes have on risk in whens, not ifs – because financial loss, business continuity, reputation and community trust are at stake.
While it's impossible to completely eliminate cyber risk, we do have good news to share. Leading FIs have proven that a more proactive approach improves their ability to avoid and mitigate risk, staying ahead of threat actors. They effectively address cyber risk from two positions:
Defense – establish a foundation that protects against current threats and prevents them from gaining a foothold.
Offense – proactively identify new threats as they arise and develop responses to them, better mitigating and avoiding risk.
Read on to discover top insights from this year's Cyber Risk Benchmarking Report.
DEFENSESTORM
THE BEST OFFENSE
A successful offense requires detailed planning, design and execution of the cyber risk playbook, which is continuously reviewed and tested. FIs can leverage internal or external resources to assist in updating their offensive playbook. About 46% of respondents conduct thorough in-house risk assessments ahead of planning and updating their program, while about 49% leverage external resources such as consultants and peer groups.
Overall, offensive planning is strong with all but 5% taking a proactive approach to advance their playbook.
These findings are in line with respondents' broader views of their offensive stance to identify and mitigate risk through systems of controls. While about 1 in 3 say they're extremely confident in their ability to manage risk, the rest (64%) could benefit from better risk identification and control design processes.
Which best describes your process for planning and implementing improvements to your program?
We conduct a thorough risk assessment prior to planning and making changes
46%
We work with consultants to help us identify risk priorities
38%
We rely on peer groups, industry associations, external trainings, etc., for guidance
11%
We make changes mostly on a reactive basis
5%
36%
are extremely confident in their ability to identify risk and design controls to effectively mitigate those risks - they have robust risk assessments and strong systems of controls
2023 Cyber Risk Benchmarking Report 12 DEFENSESTORM
Confronting fraud
It is important for FIs to employ both processes to detect cyber risk threats as well as cyber fraud threats. In a digital-first world, cybercriminals are getting better at impersonating consumers, gaining access to client accounts and escaping without a trace. Cyber fraud is a significant risk with serious impacts to an FIs bottom line and reputation. As a result, it deserves serious consideration when developing the offense component of a cyber risk program.
It's concerning, then, that 1 in 3 respondents said they depend on their cyber risk tools to detect cyber fraud despite not being designed or calibrated for fraud monitoring. Even more concerning, almost 1 in 5 only use reactive transaction monitoring tools, meaning they don't proactively monitor against cyber fraud threats. Combining traditional transaction monitoring tools with solutions specific to cyber fraud can position FIs to successfully detect and prevent fraud before money goes out the door.
How likely are you to stop cyberfraud?
Extremely likely
we have a monitoring system designed specifically for detecting and stopping cyberfraud
41%
Somewhat likely
we use a transaction monitoring fraud tool and haven't really considered what we're missing on the cyber side
18%
Very likely
we depend on our security operations to identify potential cyber fraud but the program isn't designed specifically for fraud
37%
2023 Cyber Risk Benchmarking Report 13 DEFENSESTORM

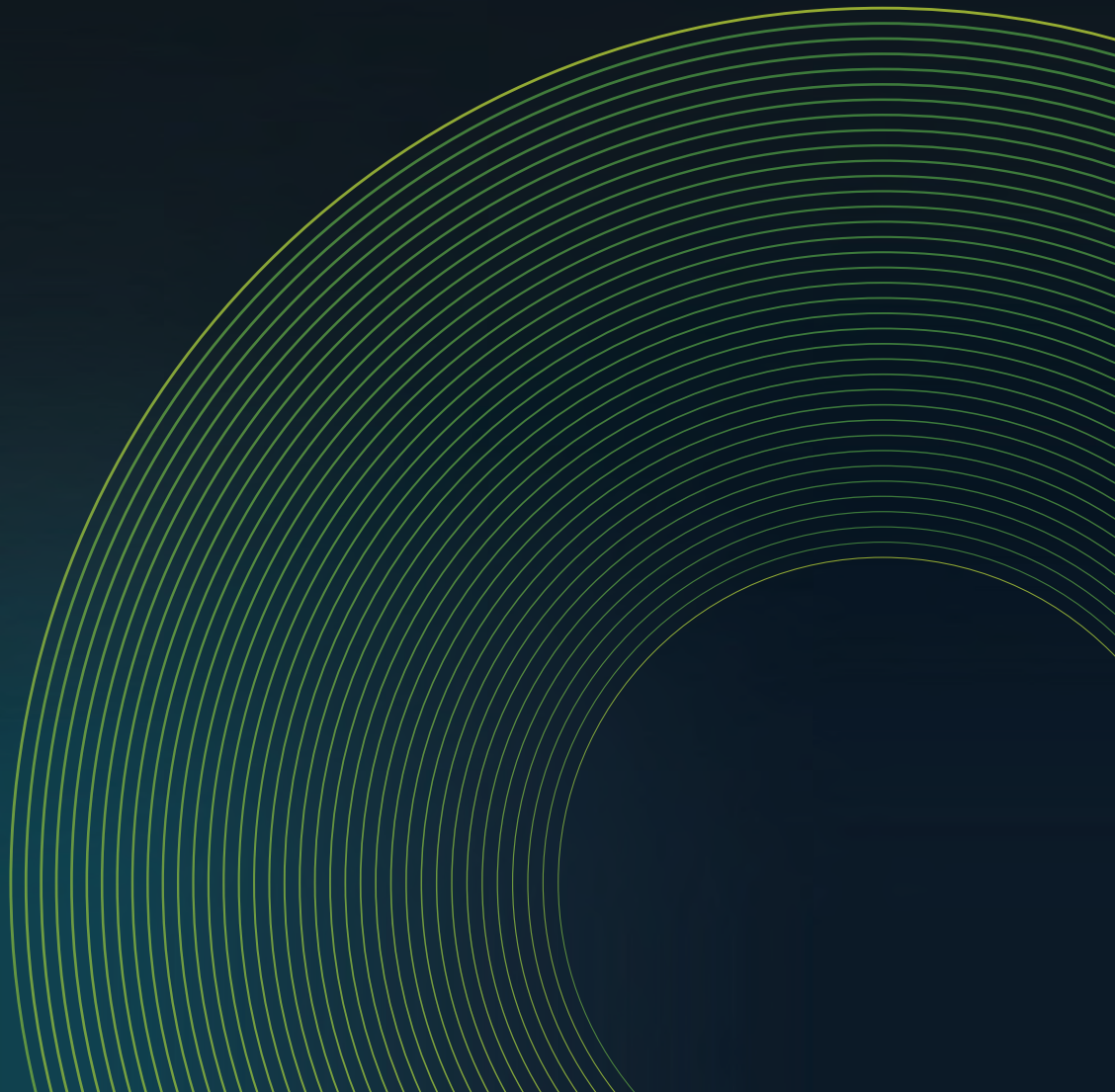
WEBSITE


DEFENSESTORM
Products
Why DefenseStorm
Resources
Community
Company
Customer Login
Contact Us
THE BEST OFFENSE.
For banks and credit unions, the financial, operational and reputational costs of waiting to combat cyber-attacks until after they happen are too great. With its dynamic nature, cyber must be treated as a risk management issue, allowing you to stay ahead of threats. That's what DefenseStorm's built for banking solution delivers.
LET US SHOW YOU
"With our prior company, all they were monitoring was server traffic and the firewall. DefenseStorm is monitoring the entire network."
That's what it means to be an ally.
Your Cyber Risk Readiness IQ
How do you measure up? Take this quick self-evaluation to determine your risk-related priorities.
2023 Cybersecurity Benchmarking Report
Protecting your institution requires a defensive and offensive approach to cyber risk management. Read how to do both.
Our Upcoming Events
Let's connect at one of our upcoming events to discuss how you can get ahead of the storm of threats.
5:24
50%
DEFENSESTORM
MENU
Customer Login
Contact Us
THE BENEFITS OF GRID ACTIVE FRAUD DETECTION
PROACTIVE MONITORING
Built for Banking, GRID Active Fraud Detection provides proactive cyber fraud monitoring and detection to stay ahead of evolving fraud threats.

ASSESSMENT TOOL

DEFENSESTORM

THE BEST OFFENSE.



QUESTIONS ON PROPER BRAND USAGE?

Contact Mia Callicutt at mia.callicutt@defensestorm.com