



STEWART ORR

PORTFOLIO 2026

I'm Stewart – a **Senior UX/UI Designer & Developer** with 25 years of experience delivering high-quality user-focused digital experiences.





2022–2025

As the sole UX/UI Designer and Developer, I played a critical role in transforming Defense.com's B2B Cyber Security SaaS product. I owned the design and development of key features end-to-end, working autonomously to introduce some of the platform's most significant functional and UX improvements.

↓ **View Highlights**





DASHBOARD

01. INTRODUCTION

The Defense.com dashboard redesign was a cross-functional UX initiative delivered in close collaboration with Product and Engineering.

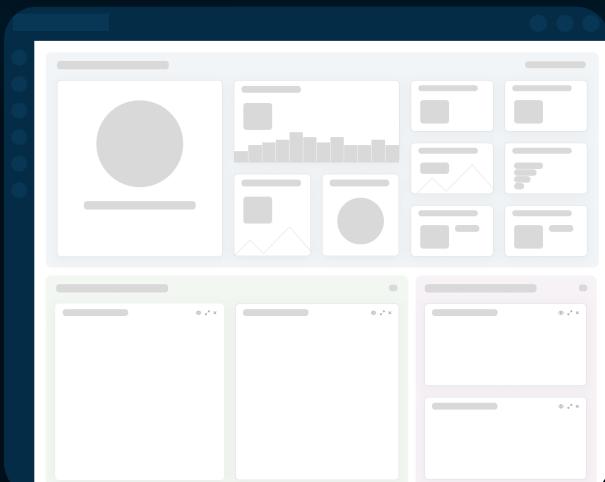
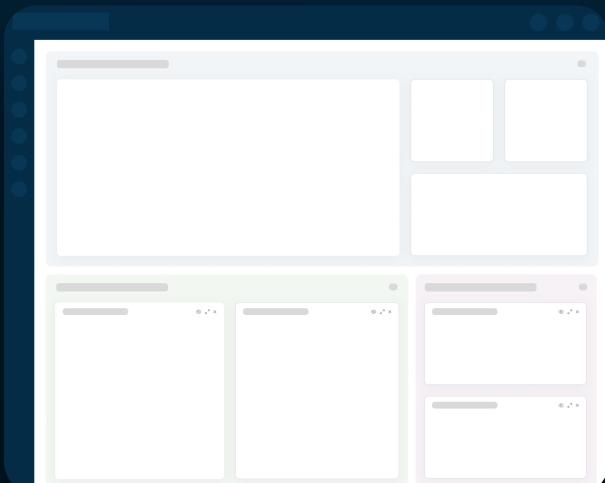
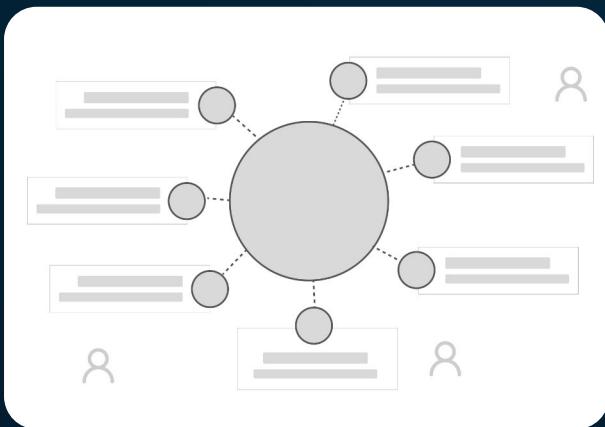
I led discovery and generative research, working with complex and fragmented threat data to understand how customers monitor, assess, and respond to security events. This included stakeholder interviews and alignment workshops to define business goals, success criteria, and the dashboard's core purpose.





DASHBOARD

02. PROCESS



Discovery

Using existing personas, I clarified primary user needs and decision-making contexts, then translated these insights into a clear information architecture and content hierarchy, defining primary, secondary, and tertiary data and the key actions users should be able to take directly from the dashboard.

Define flows & Information Architecture

As the dashboard functioned as a central hub rather than a linear journey, I focused on interaction design and user flows, mapping the routes users needed to take from the dashboard to deeper investigations and workflows.

User testing & iteration

I produced wireframes, iterating through stakeholder reviews, before developing interactive prototypes with detailed interaction and behaviour notes. These were validated through usability testing with internal analysts and a small group of customers, resulting in refinements to clarity, prioritisation, and interaction patterns.



DASHBOARD

03. RESULT



The new dashboard delivered an at-a-glance view of a customer's security posture, consolidating active threats into a single experience with a clear information architecture and content hierarchy.

The design balanced overview and depth, enabling users to quickly assess risk while supporting progressive disclosure into historical and detailed data. This allowed customers to track improvements over time, identify emerging risks, and understand whether their security posture was strengthening or deteriorating.

Designed to support customers at different stages of product maturity, the experience accommodated newly onboarded users with limited data, partially enabled users, and advanced customers seeking deeper insights.

Following launch, the solution was iteratively refined through UX measurement, combining session recordings, analytics, and user interviews to validate usability and drive ongoing improvements.

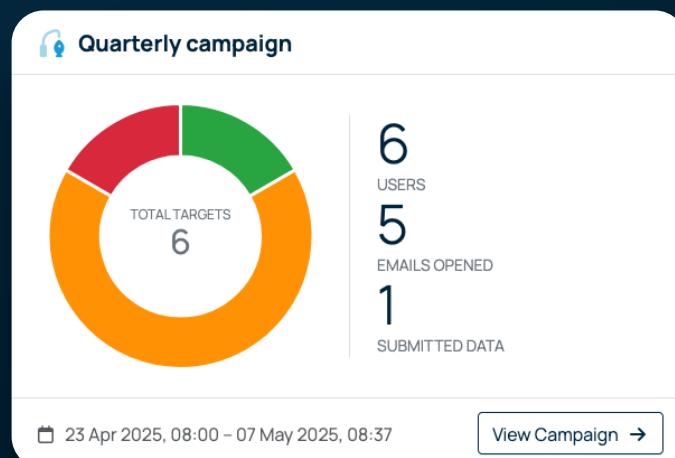


PHISHING SIMULATOR

01. INTRODUCTION

Defense.com's Phishing Simulator was significantly underutilised due to a confusing, non-visual interface and a limited set of campaign templates.

This project focused on overhauling the experience to make it more intuitive, visual, and scalable, while expanding the range of phishing templates available to customers. The redesign simplified campaign creation and significantly increased adoption and engagement with the feature.



New Campaign

Creating a Phishing Campaign

1 Select Template 2 Choose People 3 Configure 4 Review

Choose your phishing template

Select a template to use for the campaign email and landing page.

CompanyAccess
Entice your users to submit their business credentials with this password reset campaign.
Last used 26 Nov 2024 View Report >

MailDefender
Notify your users of an email held for review and see who can spot the suspicious notification.
Last used 16 Oct 2024 View Report >

Sign-a-doc
Encourage users to take action and sign up for Sign-a-doc.
Last used 11 Sep 2025 View Report >

Sign-A-Doc
Secure Digital Signing

You've been sent a document to review

Review Document

Hi there,
A document has been shared with you via the Sign-A-Doc platform for your review. Please click the link above to access the platform and review the document.

Best regards,
The Sign-A-Doc team

Please do not share this email
This email contains a secure link to the Sign-A-Doc platform.

Need Support?
Reach out to the team using support@sign-a-doc.net

Copyright © Sign-A-Doc. All rights reserved.

Campaign Preview [Email template](#) [Landing page](#)

[Select template >](#)



PHISHING SIMULATOR

02. PROCESS

The original Phishing Simulator suffered from low adoption due to limited templates and an unintuitive workflow. I collaborated with the product team to expand the available phishing campaign templates, designing email content and landing pages to support a wider range of security testing scenarios.

To support this growth, I redesigned the campaign creation experience, focusing on clarity and ease of use. I produced wireframes and interactive prototypes to explore a guided, wizard-based flow that simplified complex configuration into manageable steps.



Create Campaign

Choose your phishing template

Campaign Preview

Campaign 1 Tags: Payroll, Urgent
Last used 14 Apr, 2024 See report >

Campaign 2 Tags: Benefits, Emotive
Not used previously

Campaign 3 Tags: Benefits, Emotive

Select a campaign to get started.

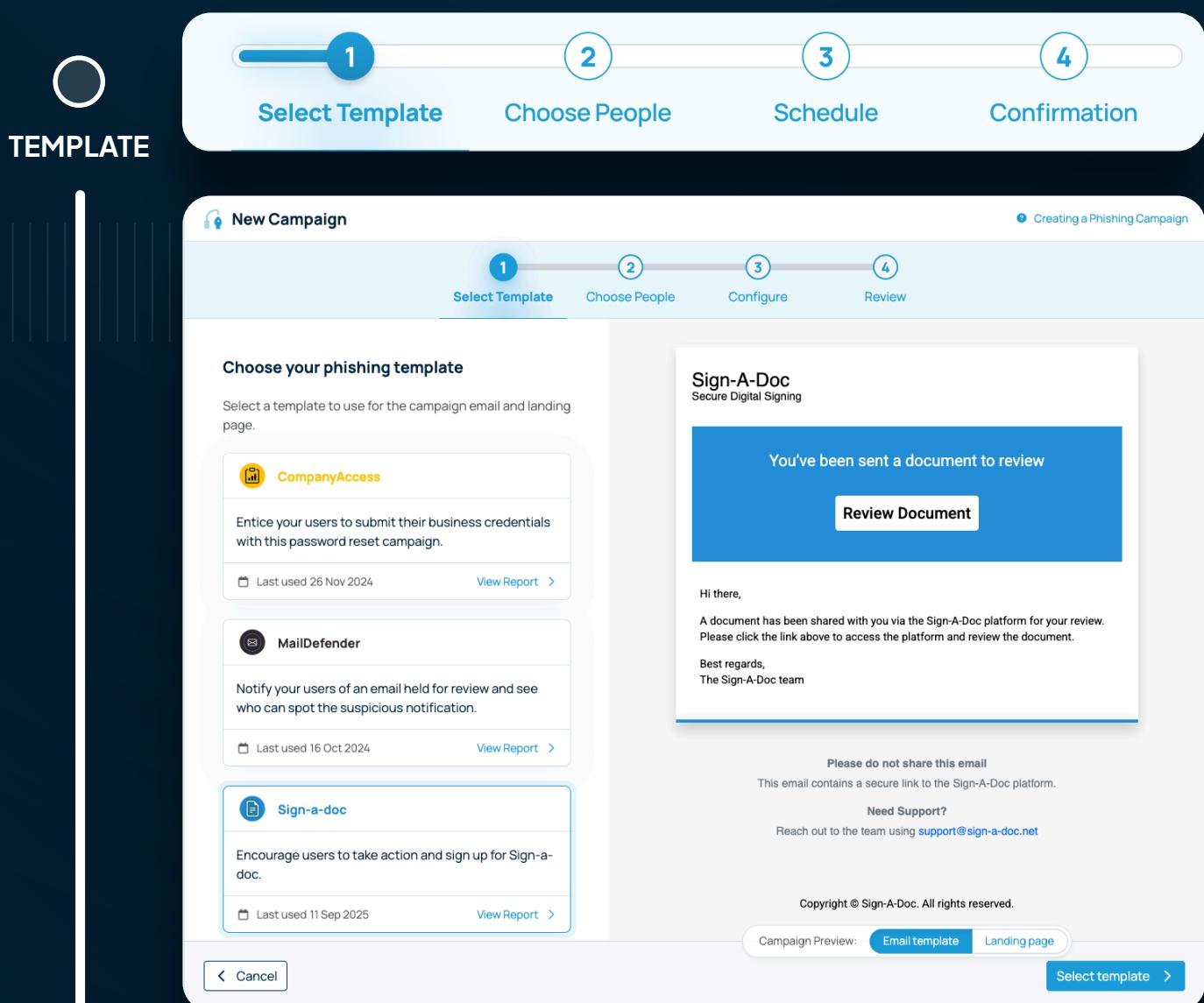
Cancel Next



PHISHING SIMULATOR

03. RESULT

Following feedback and iteration, I designed and built the final UI and front-end elements. This resulted in a substantial increase in usage and positive customer



Selecting a template allows users to preview the entire phishing campaign, switching between the email and the landing page to understand how recipients will experience the interaction.



PHISHING SIMULATOR

PEOPLE

Who should be involved in the campaign?

OP	Oliver Pinson-Roxburgh oliverpr@easyinvite.co.uk	Added	Remove
DS	Daniel Sampson daniel.sampson+demo@defence.com	Added	Remove
BC	Billy Carey bcarey@bulletproof-training.co.uk	Add	
MS	Matthew Sprague matthew.sprague+cov@bulletproof-training.co.uk	Add	
RG	Robert Garth robert.garth+dtx@defence.com	Added	Remove
SM	Sam McKee robert.mckee+dtx@defence.com	Added	Remove
R	Ruan ruan@blckrhino.com	Added	Remove
AM	Aidan Munns aidan@x5dvn.onmicrosoft.com	UNCONFIRMED	Add

[Add all users to campaign](#)

5 users selected

R	Ruan ruan@blckrhino.com	Remove
OP	Oliver Pinson-Roxburgh oliverpr@easyinvite.co.uk	Remove
DS	Daniel Sampson daniel.sampson+demo@defence.com	Remove
RG	Robert Garth robert.garth+dtx@defence.com	Remove
SM	Sam McKee robert.mckee+dtx@defence.com	Remove

[Back](#) [Next >](#)

Users who will be targetted in the campaign are then added to the test

CONFIGURE

Configure your phishing campaign

Campaign name - required

Campaign launch date and time - required

Campaign duration

We recommend you let your campaign run for a minimum of 2 weeks.

1 week 2 weeks 3 weeks

Example phishing campaign

Your campaign will run between 21 Oct 2025, 11:00 AM – 4 Nov 2025, 11:00 AM

Your campaign will run for 2 weeks

[Back](#) [Next >](#)

The campaign scheduled start and duration are selected.



PHISHING SIMULATOR

REVIEW

New Campaign Creating a Phishing Campaign

4

Select Template Choose People Configure Review

Review your campaign

Important - **sign-a-doc.net** must be added to your mail server safe senders to ensure the campaign is delivered.

Campaign template
Sign-a-doc

Campaign Name
Stewart testing

Campaign dates
Your campaign will run between 14 Oct 2025, 10:00 AM – 28 Oct 2025, 10:00 AM

Campaign duration
2 weeks

At the end of the campaign, we will report on how your users got on and we will notify you of users who failed.

5 users selected

- Ruan** ruan@blkrhino.com
- Oliver Pinson-Roxburgh** oliverpr@easyinvite.co.uk
- Daniel Sampson** daniel.sampson+demo@defence.com
- Robert Garth** robert.garth+dtx@defence.com
- Sam McKee** robert.mckee+dtx@defence.com

Finally, the campaign details are summarised and the campaign can be created.

Campaign Details

Name	Template	Status	Launch	End date
November Phishing Test	CompanyAccess	IN PROGRESS	21 Oct 2025, 11:00	04 Nov 2025, 10:00

Results Refresh

Email	Sent	Status	IP
Stewart Orr	21 Oct 2025, 11:00	EMAIL SENT	—
Susan Jacobs	21 Oct 2025, 11:00	CLICKED LINK	178.128.69.202
Tyrell Wellick	21 Oct 2025, 11:00	CLICKED LINK	178.128.69.202

User Timeline

Email	Result ID
susan.jacobs@ecorp.com	Z0pFKWW

History

- Campaign Launched 21 Oct 2025, 11:00
- Email Sent 21 Oct 2025, 11:00
- Email Opened 23 Oct 2025, 13:18
- Clicked Link 23 Oct 2025, 13:18
 - macOS (OS Version: 10.15)
 - Firefox (Version: 144.0)

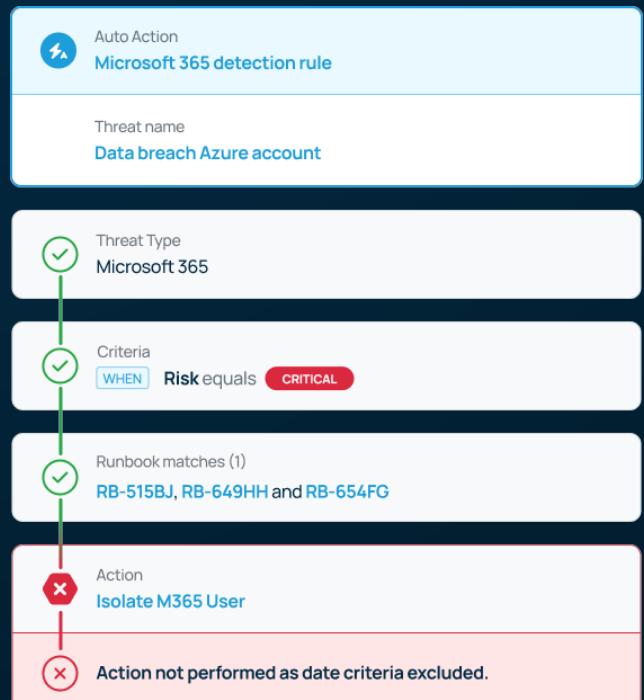
The campaign report shows progress of users targeted in the campaign.



AUTOMATIONS

01. INTRODUCTION

Automations was a new feature added to Defense.com that allowed users to create simple automated actions based on a set of rules and conditions. It was potentially a complex feature to understand so it required a UI that was quick and easy to understand.



The screenshot shows the 'New Automation' interface. The left sidebar includes 'Admin', 'Dashboard', 'Threats' (2,516), 'Assets', 'Users', 'Automations' (selected), 'Integrations', 'Penetration Testing', 'Endpoints', 'Scanning', 'SIEM', 'Education', 'Compliance', 'Account', and a user profile for 'Stewart Orr'.

The main area shows a progress bar with four steps: 'Criteria' (1/1), 'Actions' (2/2), 'Exceptions' (3/3), and 'Review' (4/4). The 'Actions' step is currently active, showing three options: 'Scan Assets' (selected), 'Isolate Assets' (selected), and 'Disable Users' (unchecked). The 'Automation Flow' section on the right shows a sequence: 'Automation example' (Automation type), 'Threat type SIEM Security Event' (Criteria), 'Runbook matches RB-Z3C-KCV Automated Recon High RB-256-G9V Automated Recon Med' (Runbook matches), and 'Action (1 of 2)' (Action).



AUTOMATIONS

02. PROCESS

Early wireframes looked to combine the process into one single screen but due to the large number of possible scenarios and the complexity of the requirements, the design was broken down into simple steps using the wizard component I designed previously.

EARLY WIREFRAME

Automated Response

Name [?](#) [How to use Automated Responses](#)

Enter your name

Criteria → **Actions** → **Exceptions**

Set the criteria for this automated response.

Threat Source

Vulnerability Scan **WHEN** Threat Risk equals Critical **AND** Assets affected greater than 50

+ AND / OR

Actions

- Disable Users: Disable all users involved in the threat.
- Isolate device: Disable all users involved in the threat.
- Scan device: Lorem ipsum dolor amet,
- Assign remediation to: Select assignee
- Auto-remediate: Fix the threat using Defense Agent.

Exceptions

When it should run

Monday-Friday

All day

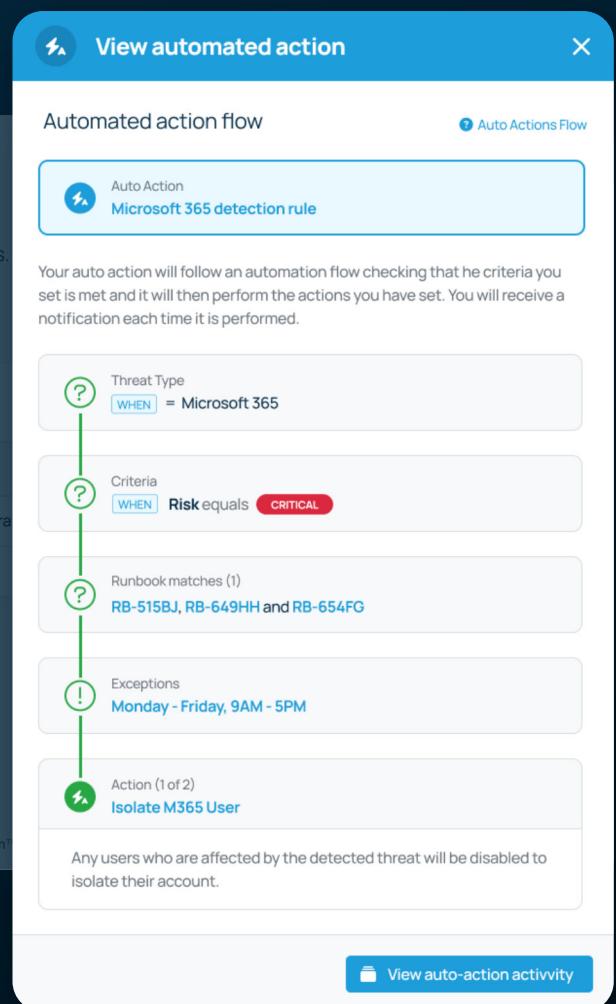
Monday-Friday

Cancel **Confirm**





As the automation will follow an ordered flow, it was important to communicate this automation flow throughout automations. I designed a simple automation flow chart that was interactive as they made changes to their criteria.





AUTOMATIONS

03. RESULT

CRITERIA

New Automation

1 Criteria 2 Actions 3 Exceptions 4 Review

Automation

Name - required
Automation example

Threat type
SIEM Security Event

Select the threat source for this automation.

Select one or more runbooks for this automation. 2 selected

Automated Recon

RB-Z3C-KCV
Automated Recon High
Quos aut accusantium. Ex sit voluptate.

RB-256-G9V
Automated Recon Med
Quos aut accusantium. Ex sit voluptate.

RB-K49-BTR
Automated Recon Low

Cancel Next >

Users start by selecting the type of threat type and selecting

ACTIONS

New Automation

1 Criteria 2 Actions 3 Exceptions 4 Review

Actions

Select one or more actions to be performed for this automation.

Scan Assets
Isolate Assets
Disable Users

Automation Flow

Automation example

Automation example

Threat type
SIEM Security Event

Runbook matches
RB-Z3C-KCV Automated Recon High
RB-256-G9V Automated Recon Med

Action (1 of 2)

Back Next >

Users can select one or more actions to be performed in the automation.



AUTOMATIONS

EXCEPTIONS

Day & Time Exceptions

Select any days/times (UTC) when you do not want the Automation to run

Sun: 09:00 - 17:00

Mon: 00:00 - 00:00

Tue: 00:00 - 00:00

Wed: 00:00 - 00:00

Thu: 00:00 - 00:00

Automation Flow

Automation example

Threat type: SIEM Security Event

Runbook matches: RB-Z3C-KCV Automated Recon High, RB-256-G9V Automated Recon Med

Time exceptions

Users can select if they would like to exclude certain dates or times.

REVIEW

Confirm

Please review your automation flow and check you are happy with the actions that will be performed.

Time exceptions: SUN 09:00 - 17:00

Action (1 of 2): Scan Assets

Any assets associated with threat detections that are not excluded will be scanned.

Action (2 of 2): Isolate Assets

Any assets associated with threat detections that are not excluded will be isolated.

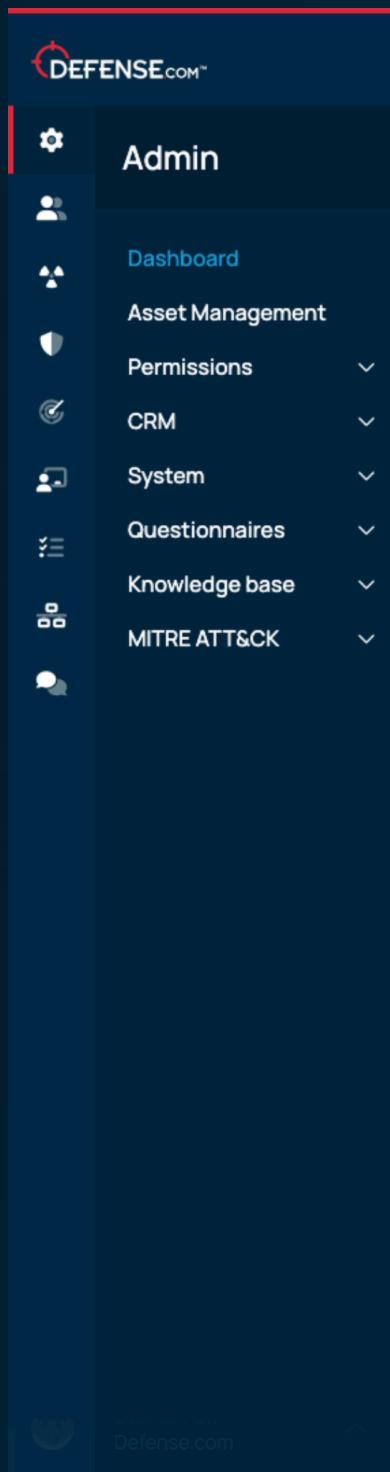
Users are finally presented with a review screen to confirm their choices and they can review the completed automation flow chart.



NAVIGATION

01. SUMMARY

The existing navigation was proving to be unintuitive for customers after several new features were added. Watching customer journeys raised a few sticking points.



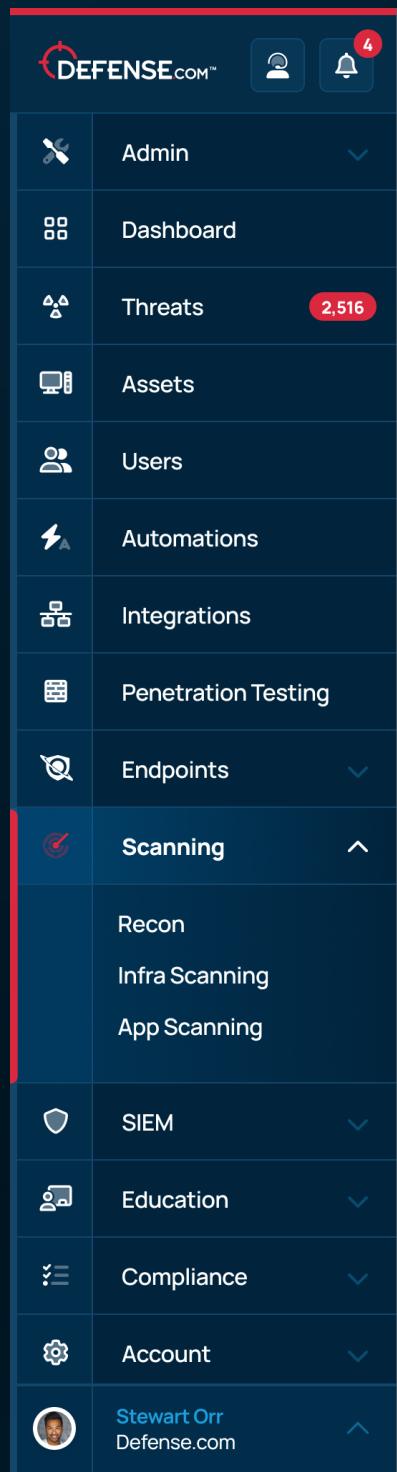
Each navigation item was now labelled to prevent the need to guess or hover the nav item.

Navigation items were rearranged in priority order for primary products features to appear first.

A threat indicator was added to draw the eye and encourage the users to take action.

Dropdown navigation items were reviewed and the group headings updated to reduce cognitive load.

The navigation was expanded to show more product features at a glance utilising the available vertical space.





DEFENSE.COM WEBSITE

01. INTRODUCTION

I was responsible for the Defense.com website which involved designing and building new content and optimising for accessibility, conversion and performance. I developed a Design System and Component library for regular components for the website that were thoroughly tested and optimised across different devices and browsers.

The healthcare industry is under attack.

- ✓ **41% of health care organisations** reported experiencing a cyber security breach or attack in the last 12 months.
- ✓ In 2024 a **major ransomware attack** led to the postponement of 1,693 elective procedures and 10,054 acute outpatient appointments at key NHS trusts.
- ✓ Phishing is the root cause of **85% of breaches** in health care organisations.

Ready to strengthen your Defences?

First name * Last name *

Business email * Phone number

Company name *

What are your security challenges or concerns?

Keep me informed: I consent to receive news, updates, and promotions. For more information about how we collect, process and retain your personal data, please see our [privacy notice](#).

How Defense.com can provide much-needed support

Defense.com offers a comprehensive suite of cyber security tools designed to detect, prevent, and respond to threats efficiently. Our platform is trusted by over 4,000 businesses worldwide, with proven success in the healthcare industry.

Trusted by industry-leading healthcare providers

NHS North London NHS Foundation Trust BrisDoc MED-E-CARE

Healthcare professionals are on the front line

Healthcare providers are on the front line of invaluable, and breaches can lead to severe consequences. At Defense.com, we specialise in solutions tailored to the unique needs of the organisations like the NHS stay secure and compliant.

Seamless Integration with Existing Tools

Our platform integrates effortlessly with your existing security investments, including Endpoint Detection Response tools, network security systems and more. This ensures you can enhance your defences without the hassle of overhauling your setup, saving valuable time and resources.

Unified Threat Management

Our advanced threat management system consolidates alerts and insights into a single interface, providing complete visibility across your network, endpoints, and cloud environments. This eliminates the need to hop between systems, enabling rapid threat detection and response for busy healthcare teams.

Managed Detection and Response (MDR)

Benefit from 24/7 monitoring by our expert Security Operations Centre (SOC) analysts, who proactively investigate and neutralise threats, ensuring minimal downtime for your operations.

Instant Mitigation Strategies

Every threat comes with AI generated step-by-step, practical advice for remediation, tailored to your environment.



DEFENSE.COM WEBSITE

02. HIGHLIGHTS

UX was continuously monitored using analytics tools and customer journey tools like Google Analytics and Mouseflow with improvements regularly being made.

The landing page features a prominent sign-up form with fields for First name, Last name, Business email, Phone number, and Company name. A note below asks for security challenges or concerns, with a checkbox for staying informed about news, updates, and promotions. A 'Speak to us' button is at the bottom.

The 'Integrations' page highlights the ability to seamlessly integrate essential security tools. It features a network diagram with a central 'DEFENSE.com' node connected to various cloud and endpoint icons. Below is a grid of 20 integration icons, each with a 'View details' button.

Trusted by leading education providers: Logos for YORK ST JOHN UNIVERSITY, LOUGHBOROUGH Schools Foundation, TRINITY COLLEGE CAMBRIDGE, PEMBROKE COLLEGE OXFORD, and YORK ST JOHN UNIVERSITY.

Safeguard Your Students and Staff with Defense.com: A photo of students in a classroom. Text: Educational institutions, from schools to colleges and universities face escalating cyber threats. Sensitive student data, online learning platforms, and interconnected networks make the sector a prime target for cybercriminals. At Defense.com, we provide comprehensive cybersecurity solutions tailored to the unique needs of education, ensuring you can focus on inspiring the next generation without the worry of security breaches.

Growing Cyber Threat in Education: A photo of a student using a computer. Text: Cyber attacks on educational organisations are on the rise, disrupting learning and causing sensitive information. The figures below underscore the vulnerability of the sector, with potential impacts including lost learning time, financial costs, and reputational damage. Don't let a cyber incident derail your organisation's mission. Proactive protection is essential.

Why Education Organisations Choose Defense.com: A section with three cards: 1. A chart showing 73% of UK educational institutions have experienced at least one cyber-attack or breach in the past five years. 2. A card showing 215 personal data breach reports between January 2022 and August 2024 in the education sector caused by insider threats. 3. A card with a red background and white text.



DEFENSE.COM WEBSITE

02. HIGHLIGHTS

DEFENSE.COM™

Platform ▾ Managed Services ▾ Solutions ▾ Pricing Partners Resources ▾ Try for free

Expert knowledge at your fingertips

Keep up to date with the latest news & announcements at Defense.com

Tags: [Events](#) [Product & Tech](#) 14 [Risk & Compliance](#) 12 [Security Advice](#) 20 [Threat Maps](#)

Check out our latest blogs

Risk & Compliance

Cyber Security and Resilience Bill: Why Your Business Can't Wait

The UK government's new UK cyber law brings massive fines, mandatory CAF compliance, and 24-hour incident reporting. Even small suppliers can be designated critical and brought into scope.

Product Update May 2025 Webinar

Event Detection & Response for Your Business. Secure

Discover more about SIEM

DEFENSE.COM™

Platform ▾ Managed Services ▾ Solutions ▾ Pricing Partners Resources ▾ Try for free

Cyber Security Glossary

From APT to XDR, cyber security can be a minefield of terms and acronyms. Here's our ultimate definitions guide to make your life a little easier.

Search our glossary...

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Filter by topic: Endpoint Cyber attacks Malware Security Social engineering SOC/SIEM Scanning

Adware Endpoint Cyber attacks Social engineering

Adware is software designed to display various pop-up advertisements on your computer or mobile device. It has the potential to become malicious and harm your device by slowing it down, hijacking your browser and installing viruses and/or spyware.

AEP - Advanced Endpoint Protection Endpoint SOC/SIEM Scanning

Advanced Endpoint Protection (AEP) is a cyber security counter measure that uses machine learning and other threat intelligence to detect and block anti-virus, anti-malware, and anti-spyware software. Threats are detected and blocked based on anomalous behavior by the machine learning algorithm, which is trained to detect patterns in the log files and monitor the system for unusual activity.

AI - Artificial Intelligence SOC/SIEM Cyber attacks Scanning

Artificial Intelligence (AI) is a field of study that deals with the theory and development of artificial intelligence and its application in the creation of machines and software that can exhibit intelligent behavior. AI in cybersecurity will be an advanced form of machine learning that can train itself to act autonomously to identify and stop cyber threats resulting into a low-touch, high-impact security system.

Angler Phishing Cyber attacks Social engineering

Angler phishing is where social media accounts are set up which act under the pretense of customer support to extract personal information. Victims are lured in by being prompted to click a suspicious link that installs malware to your device.

Anti-Malware Software Scanning

Anti-malware software identifies, prevents, and removes malicious software using a scanner. It can detect known malware by comparing suspicious files against a database of previously identified malware signatures. Anti-virally behavior based anti-malware software will check if a program looks suspicious and flag it to the user even if it doesn't match a known virus. Users are often confused about the terms anti-virus and anti-malware, but generally, the products are the same and anti-malware is simply a more recent term.

Anti-Virus Endpoint Scanning

Originally produced to protect PCs from malicious software, anti-virus has evolved from using one dimensional signature virus recognition to a multifaceted approach seen today in sophisticated scanning software, which uses predictive analytics, machine learning and AI capabilities.

Anti-Virus Software Endpoint Scanning

Anti-virus software, also known as anti-malware, is a type of computer program which was initially designed to identify, prevent, and remove computer viruses. Modern anti-virus protects against a variety of malicious tools such as keyloggers, ransomware, rootkits, browser helper objects (BHOs) and trojans.

Asset Endpoint

An asset is any data, device or other component of an organization's systems that contains sensitive data or can be used to access such information. Tangible assets include smartphones, laptops, tablets and PCs, which are often connected to company networks, making them a target for cyber criminals. Virtual assets include databases, file servers, email servers and third-party cloud storage systems.

Asset Profile Endpoint

Assets define your attack surface, therefore it's essential to understand how they could become targets. An Asset Profile is a tool which maps threats directly to your unique list of hardware and operating systems, making it simple to gather, prioritize and action threat intelligence data.

ATO - Account Takeover Attack Cyber attacks Social engineering

Account takeover attacks are a type of cybercrime where the attacker gains control of an account by stealing login credentials, guessing passwords, or using social engineering to persuade the victim into revealing their sign-in information.

Attack Signature Malware

An attack 'signature' is a set of characteristics and behaviors that help identify, detect, and defend against specific types of cyber-attacks and is commonly used by antivirus software to identify and isolate known viruses and malware. This enables security software to block attacks before they can cause any damage, by analyzing the patterns of attack and the protocols used to send alerts to the operating system.

Attack Surface Cyber attacks

The attack surface refers to the various points of entry where an unauthorized user may enter or extract data from an environment. Keeping the attack surface as small as possible is a security best practice that can help protect your data and systems from a cyber attack.

Automated Cyber Attacks Cyber attacks

Automated cyber attacks are carried out by machines which are programmed to run without any human input and have become more common in recent years because they can be done faster and more efficiently than manual hacks. There is also less chance of being caught since the person who programmed the bot does not need to be present for it to work.



BULLETPROOF

01. INTRODUCTION

Bulletproof offer cyber security and data protection services and their website looks to convert users who need those services by showing trust signals and expertise throughout their website.

Expert cyber security services
from a trusted cyber security company

Solving problems with simplicity & innovation to make compliance & cyber security services accessible to everyone.

Why choose us?

Continuous Security Protection

Protect your business 24/7 with automated scans included with every penetration test.

Competitive Pen Test Prices

Bulletproof prices are highly competitive without sacrificing quality, keeping you protected.

Get in touch

Helping people solve their security challenges is what we do, so we're always keen to hear from you, no matter what you have to say.

Benefits of penetration testing

Uncover your security weaknesses

Penetration testing uses human skill & insight to uncover threats.

Automated security scans

Continuously uncover the latest threats to your business.

Get a quote

01438 500 093

Get a quote

Cyber Security Jargon Buster

A helpful index of cyber security terms including common compliance acronyms and pen test terminology.

A B C D E F G H I J K L

Access Control

Access control is a security technique that helps organizations to control individual access to business data by authenticating

Get a quote

Unit H, Gateway 1000, Whittle Way, Stevenage, Herts SG1 2PF

01438 500 093

contact@bulletproof.co.uk

Get a quote

Company

Data Protection

Penetration Testing

Information Testing

Information Security

Resources

© 2026 Bulletproof. All rights reserved.

Terms Privacy Cookies Vulnerability disclosures

Appropriate policy document



BULLETPROOF

02. FOOTER

The website footer was redesigned to focus on user navigation making it simpler by grouping and listing all services offered by Bulletproof and to put core pages at a glance. The style was updated to match the brand styling.

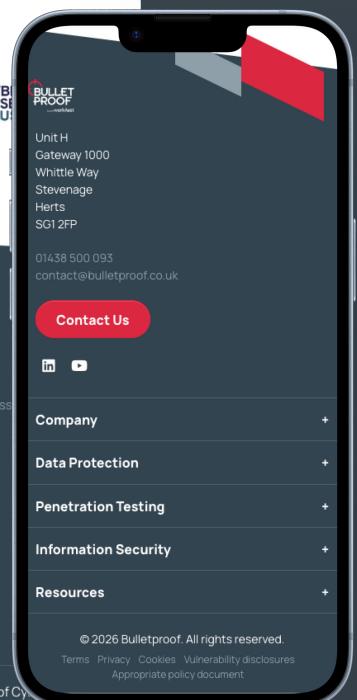
OLD

© 2016-2025 Bulletproof.co.uk. All rights reserved.

Bulletproof is a trading name of Defense.com Cyber Ltd.

NEW

Trusted cyber security & compliance services from a certified provider



Unit H
Gateway 1000
Whittle Way
Stevenage
Herts
SG12 7FP
01438 500 093
contact@bulletproof.co.uk

Contact Us



© 2025 Bulletproof. All rights reserved.

[Terms](#) [Privacy](#) [Cookies](#) [Vulnerability disclosure](#) [Appropriate policy document](#)

Bulletproof is a trading name of Bulletproof Cy

Company number 05490180 • VAT number 865563391

© 2026 Bulletproof. All rights reserved.
Terms Privacy Cookies Vulnerability disclosures
Appropriate policy document



BULLETPROOF

03. HEADER & NAVIGATION

The navigation was redesigned and updated to become a mega nav. Structured into different product service categories, this meant users could quickly explore and navigate to the services they required quickly.

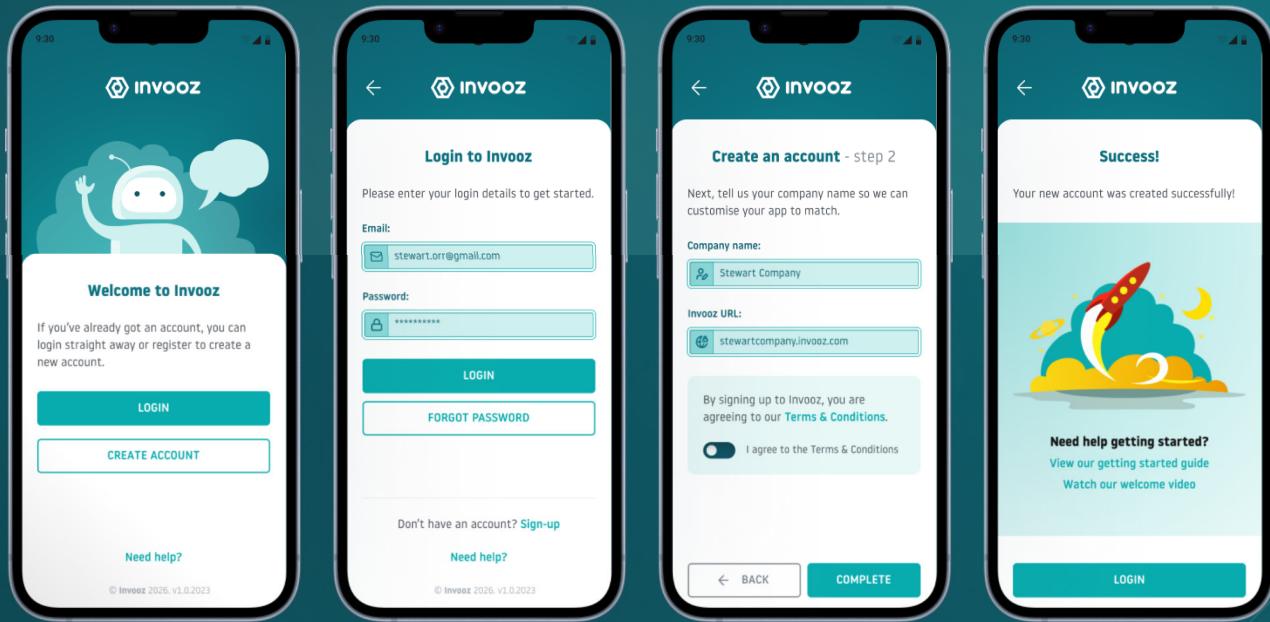
OLD

NEW



 Invooz

Invooz is an invoicing and time management tool that makes it easy for users to manage customers and create invoices easily. I designed the brand, mobile application and web application and built the web application.



The dashboard displays the following key metrics:

- INVOICES:** £4,820 (up +11.48% this month)
- INVOICES:** 2 (up +11.48% this month)
- TOTAL:** 61 contacts (158 contacts)
- CLIENTS:** 61 contacts (158 contacts)

Below the metrics, the **DASHBOARD** section shows the status of invoices:

- 1 DRAFT
- 0 PENDING
- 1 SENT
- 0 DUE
- 0 LATE
- 0 PAID

A line chart at the bottom tracks the volume of invoices issued monthly from January to December, comparing two financial periods: 2020/2021 (light blue) and 2019/2020 (dark blue). The chart shows significant peaks in June and November, with a notable dip in September.



INVOOZ

Hello, Array. [Profile](#) [Help](#) [Log out](#)

[DASHBOARD](#) [CLIENTS](#) [INVOICES](#) [ACCOUNT](#)

[CLIENTS](#) [Create new](#) [Search](#) [Help](#) [More](#)

ALL 0-9 A B C D E F G H I J K L **M** N O P Q R S T U V W X Y Z

Showing 7 client(s) beginning with M — page 1 of 1

M	Client Name	Website	Invoices	Contacts	Address	More
	Made Purple Ltd	www.madepurple.com	19 invoices	1 contact	Keystone Innovation centre, Croxton road, Thetford, IP24 1JD	
	Marks and Spener plc	www.marksandspencer.com	25 invoices	15 contact	NO157005 Non Merchandise Payments, 8th Floor, 3 Hardman Street, Spinningfields, Manchester, M3 3HF	
	Maxim Design Consultants	themaxuk.com	2 invoices	1 contact	Wheatheaf House, 39 High Street, Wheathampstead, Herts, AL4 8BB	
	Megaman (UK) Limited	www.megamanuk.com	98 invoices	12 contact	Megaman House, 2 Quadrant Park, Mundells, Welwyn Garden City, Herts, AL7 1FS	
	Megaman Lighting Australia Pty Lt	www.megamanlighting.com.au	5 invoices	2 contact	64/60-82 Princes Highway, St Peters, Sydney, NSW 2044	
	Mohican Mole	www.mohicanmole.com	2 invoices	2 contact	The Old House Farm, Oddley Lane, Saunderton, Nr Princes Risborough, Bucks, HP27 9NQ	
	Monsters Edge Ltd	www.monstersedge.com	16 invoices	1 contact	17 General Business Park, Bury St Edmunds, Suffolk, IP22 4JL	

CALENDAR

JANUARY FEBRUARY 2026 MARCH 2026

MON	TUE	WED	THU	FRI	SAT	SUN
2	3	4	5	6	7	
9	10	11	12	13	14	
16	17	18	19	20	21	
23	24	25	26	27	28	

DASHBOARD

1 DRAFT 2 PENDING 3 SENT 1 DUE 2 LATE 31 PAID

120
100
80



OPPORTUNITY INTERNATIONAL

WHAT WE DO.



Opportunity International provides people living in poverty with access to loans, financial training and savings so that they can work their way out of poverty and build sustainable livelihoods. We give people a hand up not a handout. A simple opportunity enables people to grow their income and build a secure home where their children can have regular meals, attend school and work towards a better future.

We focus on three programme areas – Enterprise, Agriculture and Education- which serve Women, Farmers, Refugees, Young People, Schools and People living with disabilities.

[What we do](#)

5,000 refugees in Uganda.

Sed viverra porta suscipit. Nunc nec volutpat dolor. Aliquam erat volutpat. Sed ac erat et neque ultrices venenatis. Donec pharetra eu mauris ut tempor. Duis tristique lectus at arcu ornare facilis. Phasellus egestas massa vitae felis placerat, rutrum euismod leo scelerisque. Pellentesque molestie luctus urna, quis commodo metus tempus sed.

97%

of our loan clients are women

1.87 MILLION

clients working their way out of poverty

3.5 MILLION

children benefiting from our education programme

Leila.



Country: Ghana

Leila is a farmer from rural Ghana. With no formal training or access to the resources needed, her farm barely produced enough to feed her family, let alone extra to sell. A loan, alongside agricultural and financial training from Opportunity International, enabled Leila to buy fertiliser and farm more efficiently so that she dramatically improved the farm's productivity.



Leila has been a farmer most of her life. Her father died when she was young, which meant she could no longer go to school and had to help her mother on their farm.

She is a wife and mother to three young children. Before she met Opportunity International, Leila was struggling to make ends meet on her farm. She had no formal training or access to the resources she needed. Her farm barely produced enough to feed her family, let alone extra to sell.



Leila is part of a community group of local farmers. Opportunity International provided Leila and her group with training in finances and agriculture, helping them to save securely and improve their farming.

“

At first, I didn't know that when we farm we are meant to save part of our money. We were taught how to get the best quality from our land and how to save.



MEGAMAN®

I designed and developed Megaman UK's website presence for over 8 years. It had grown from a simple 10 page site to a large content managed site with over 2,500 pages and products with several intuitive tools to help customers choose Megaman products.

MEGAMAN®

Search the site

[ABOUT](#) [PRODUCTS](#) [AUDIENCE](#) [MEDIA](#) [DOWNLOADS](#) [SUPPORT](#) [CONTACT US](#)

[Twitter](#) [Facebook](#) [YouTube](#) [LinkedIn](#)

Performa
Fixture Range

710709

[Home](#) > [PRODUCTS](#) > [PERFORMA | LED FIXTURES](#) > [MILENA](#) > 710709



MILENA Integrated DUAL CCT LED Downlight 6W/8W 3000K or 4000K Switchable
SKU: 710709



A cost-effective and ideal replacement for traditional PL commercial downlights, MEGAMAN®'s MILENA is a compact integrated LED downlight perfect for use directly under thermal insulated ceiling recesses.

[Specifications](#) [Features](#) [Downloads](#) [Where to Buy](#)

Specifications

MILENA Integrated DUAL CCT LED Downlight 6W/8W 3000K or 4000K Switchable	
Product Code	710709
International Model Number	FDM70700v0-ds/00
Description	Integrated DUAL CCT LED Downlight
Watts	6W/8W
Colour Temp	3000K or 4000K
Lumens	400lm
Lamp life L70	50,000 hours
Lamp life L80	30,000 hours
Dimensions	115mm x 65mm
IP Rating	IP44
Colour/Finish	White
Dimmable	Yes
Hole cut out	65mm
Beam Angle	120°
Operating Temperature	-20°C to 40°C

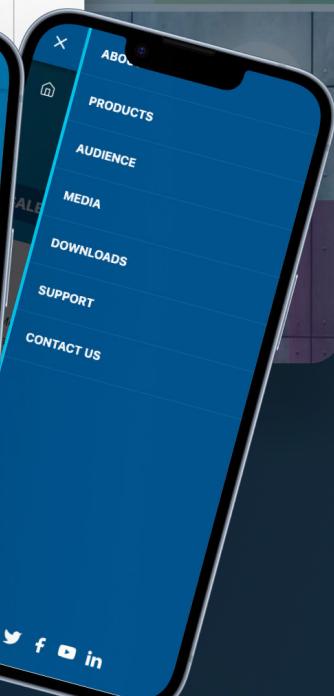
[Back to MILENA](#)

ALTERNATIVE PRODUCTS


710689
MILENA Integrated DUAL CCT LED Downlight 18W/24W 3000K or 4000K Switchable [NEW](#)


710691
MILENA Integrated DUAL CCT LED Downlight 20W/27W 3000K or 4000K Switchable [NEW](#)







MEGAMAN®

COST OF OWNERSHIP TOOL

Megaman wanted an new tool that helped potential customers realise the savings of switching from traditional halogen lighting products to their energy efficient LED range. The **Cost of Ownership** toolv allowed the customer to create a report that demonstrated the savings based on their existing products and usage.

MEGAMAN®

Search the site

ABOUT PRODUCTS AUDIENCE MEDIA DOWNLOADS SUPPORT CONTACT US

COST OF OWNERSHIP TOOL

SALES SUPPORT > COST OF OWNERSHIP TOOL

This cost of ownership calculator is intended to provide an illustration of potential savings when you switch from your current non-energy saving products to Megaman LEDs based on the data you input. Actual savings may vary. The LED lamp option that appears in the first column, marked as the true replacement is the most suitable direct replacement for your current product. The specification of the other alternatives may differ slightly compared to your current product with regards to output, lamp life or dimming capability.

1 Current products **2 Current usage**

Megaman's Cost of Ownership Tool

Choose the lamp you wish to replace from the below selection.

That product was already in your list.

12 35W Halogen GU10 25 50W Halogen AR111

You could save up to £94.79 per year

Email report **Download report** **Find nearest stockist**

Add product

Select the product you are looking to replace with a Megaman LED alternative.

GU10-Spot **GLS-Classic-Bulb** **Candle** **AR111**

Your savings

Below is a list of Megaman energy efficient LED alternatives to the current lamp(s) you are using. Savings are based on the quantity of lamps and your daily / weekly usage specified in the previous stage. Remember you can save this report as a pdf for future reference or find your nearest Megaman LED stockist.

You could save up to £94.79 per year

15 x 35W Halogen GU10

By switching to a Megaman energy efficient LED you could save up to £94.79 a year in energy costs, 368 Kg a year in CO₂ and it will last up to 12 times longer.

Based on your usage 4 hours a day, 7 days a week costing £0.14p/kW an hour.

Product	CURRENT PRODUCT	TRUE REPLACEMENT	ALTERNATIVE OPTION	ALTERNATIVE OPTION	
Order code	-	141730 2800K 141732 4000K	141724 28000K 1417269 40000K 141728 6500K	141322 2800K 141324 4000K	
Price	-	£45.00	£3.00 x 15	£67.50	£4.50 x 15
Wattage	35W	4W	5.5W	5W	14W
Lamp life	2,000 hours	25,000 hours	50,000 hours	25,000 hours	
Annual energy cost	£107.02	£12.23	£16.82	£15.29	
Annual saving	-	£94.79	£90.20	£91.73	
Estimated payback	-	5 month(s)	1 year(s) 3 month(s)	8 month(s)	
Annual energy	764 kW	87 kW	120 kW	109 kW	
Annual CO ₂	416 Kg	48 kg	65 kg	59 kg	
Lumens	-	250	500	360	
Dimming	-	No	Yes	Yes	
Change product	-	Choose product	Choose product	Choose product	

Summary

Current products: 15 x 35W Halogen GU10

Current usage: 35W Halogen GU10 - 4 hours a day, 7 days a week.

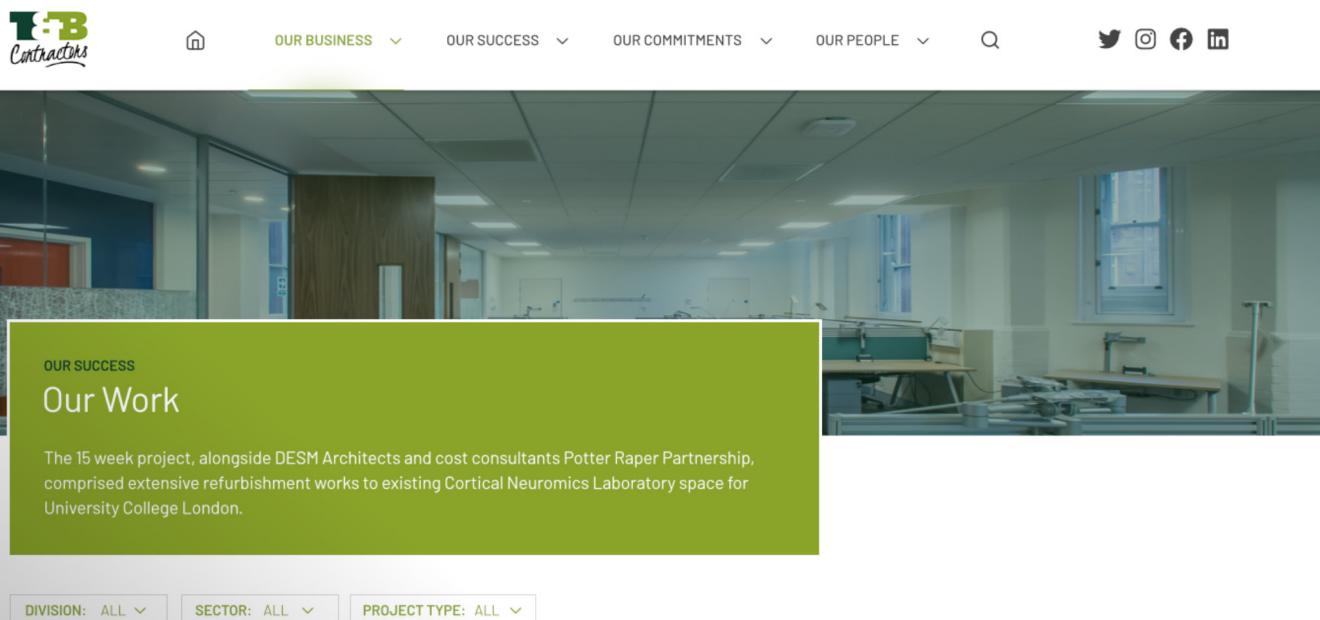
Your savings: Estimated savings over the life time of the LED replacement(s). £94.79

Email report Download report Find nearest stockist



T&B CONTRACTORS

I've worked with T&B Contractors for several years and was asked to redesign their website to modernise and exhibit their construction projects. The site was built responsively and was content managed so they could make their own changes and add future projects.

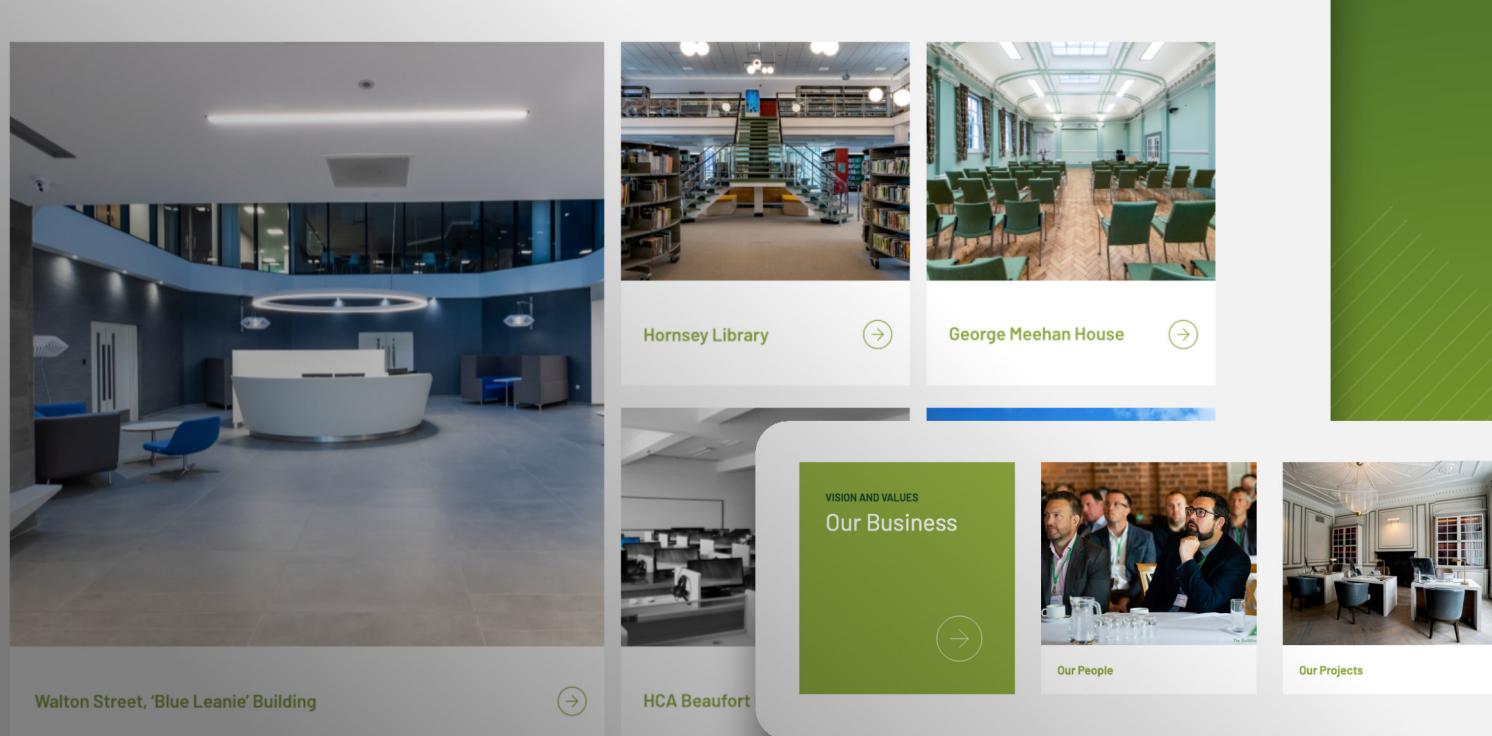


OUR SUCCESS

Our Work

The 15 week project, alongside DESM Architects and cost consultants Potter Raper Partnership, comprised extensive refurbishment works to existing Cortical Neuromics Laboratory space for University College London.

DIVISION: ALL ▾ SECTOR: ALL ▾ PROJECT TYPE: ALL ▾



Walton Street, 'Blue Leanie' Building

Hornsey Library

George Meehan House

HCA Beaufort

VISION AND VALUES

Our Business

Our People

Our Projects



OUR BUSINESS OUR SUCCESS OUR COMMITMENTS OUR PEOPLE

Discover More
Our Projects

OUR WORK
UCL - Cortical Neuromics Laboratory

The 15 week project, alongside DESM Architects and cost consultants Potter Raper Partnership, comprised extensive refurbishment works to existing Cortical Neuromics Laboratory space for University College London.

01-02
Harcourt House, Marylebone The Abbey School, Faversham West London College, Southall Keppel St

[Explore projects →](#)

01

The Project

DIVISION

Contracting

CLIENT

University College London

PROJECT

Cortical Neuromics Laboratory

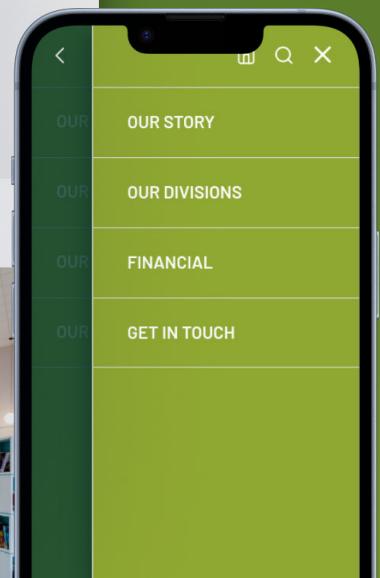
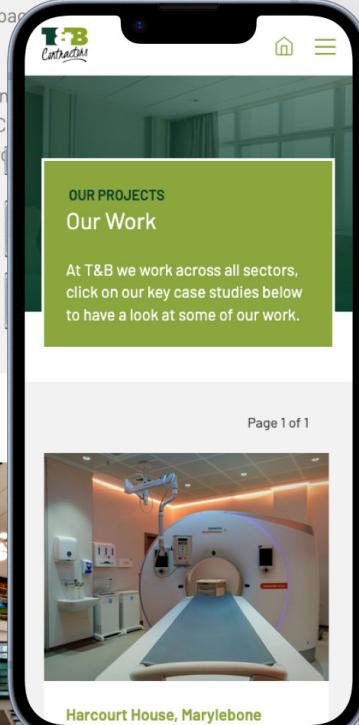
CONTRACT VALUE

£700,000

CONTRACT DURATION

24 weeks

The 15 week project, alongside DESM Architects and cost consultants Potter Raper Partnership, comprised extensive refurbishment works to existing Cortical Neuromics Laboratory space for University College London.





MOTREMIND.ME

One of my own project sites which sends MOT reminders by email to users who register. It also has a directory listing of all MOT Test Centres in the UK that users can browse and or search using geolocation.



purple visits

purple visits

HOME

ABOUT

HELP

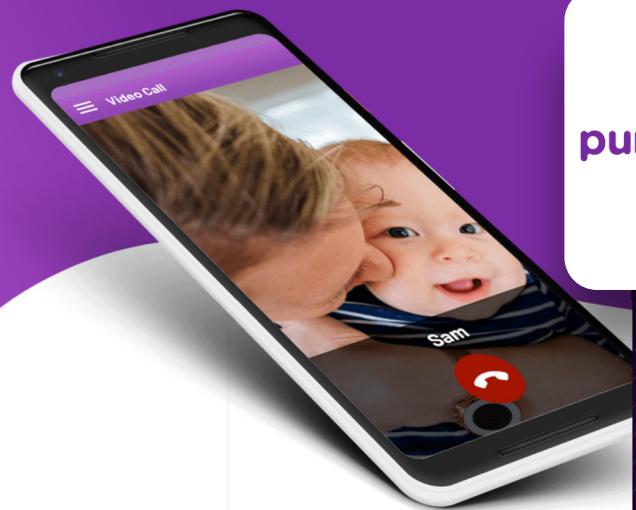
CONTACT

DOWNLOAD

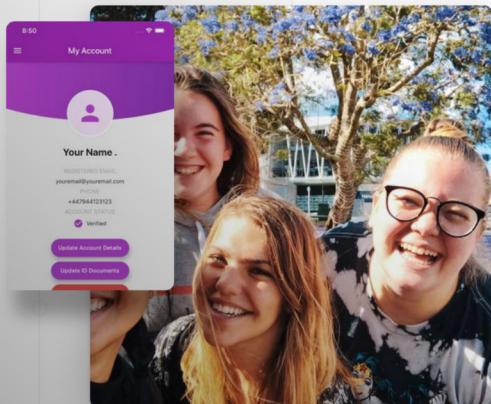


Secure video calling
from the comfort of
your own home.

DOWNLOAD

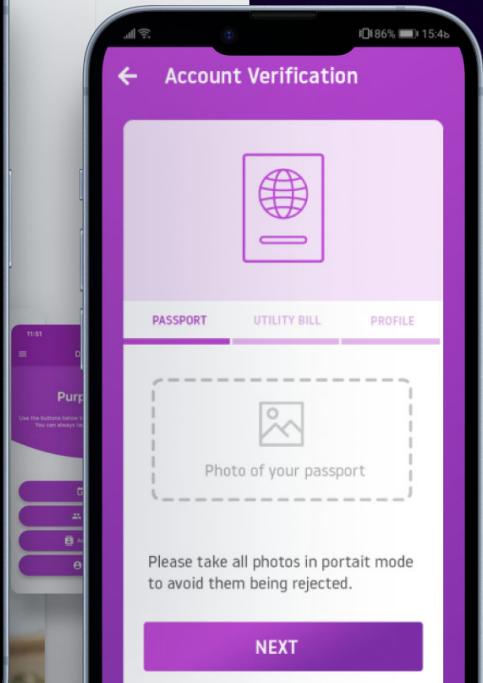
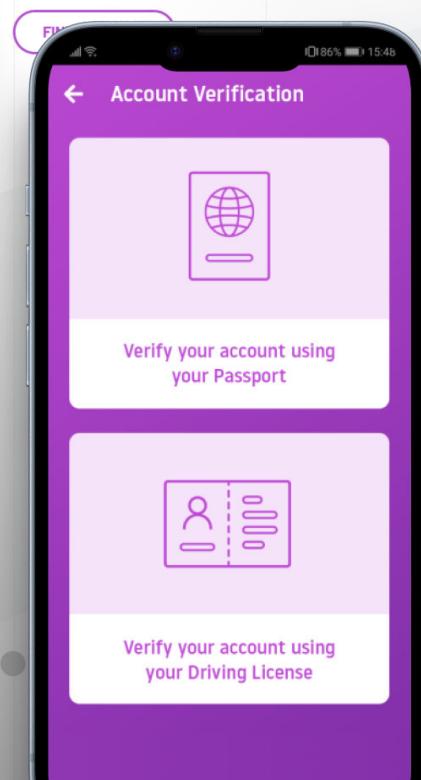


purple visits



Secure, reliable video calling

Lorem, ipsum dolor sit amet consectetur adipisicing elit. Natus distinctio illum ut nobis voluptas laudantium suscipit? Quia, reprehenderit! Aut minima optio delectus nisi quibusdam reiciendis, in sint cum inventore voluptates.



HD Video Calling using WiFi & 4G

Our unique compression system means that even people with low speed broadband can use Purple visits.

FIND OUT MORE



e3light.®

e3light. light that matters

CONTACT US



uksales@e3light.com



01707 243430



01707 243430



www.e3light.co.uk

E3LIGHT LTD
UNITS 2/4
LITTLE RIDGE INDUSTRIAL ESTATE
WELWYN GARDEN CITY
HERTS
AL7 2BH

T: +44 (0) 1707 243430
F: +44 (0) 1707 243431
E: uksales@e3light.com
W: www.e3light.co.uk



GET IN TOUCH

LOREM IPSUM DOLOR SIT AMET, CONSECTETUR ADIPISCING ELIT. MORBI INTERDUM EU NIHIB SED LACHNIA. NUNC TRISTIQUE RISUS LEON, ID CONSECTETUR IPSUM EGESTAS PORTA.

NAME

I'M INTERESTED IN

momit Energy Eye Voltaware MyLight

EMAIL

ENQUIRY

SEND MESSAGE

momit
Smart technology for everyone

WELCOME TO THE SMART WORLD.

THE CONTROL IS YOURS. MOMIT FINDS YOUR MAXIMUM COMFORT GIVING YOU THE OPTION TO CONTROL EVERYTHING FROM YOUR HOME TEMPERATURE TO YOUR MONTHLY EXPENDITURE. BEST OF ALL, YOU CAN DO IT EASILY FROM ANY MOBILE DEVICE OR SMARTPHONE.



MOMIT HOME THERMOSTAT MOMIT SMART THERMOSTAT MOMIT COOL MOMIT BEVEL

momit
BEVEL

PERFECT TEMPERATURE IN ANY ROOM

MOMIT BEVEL



CONTROL FROM THE APP
Control momit Bevel through your mobile device.

CONTROL HEATING
Control the boiler or floor heating from the app.

MY BUDGET
Decide your monthly energy bill.

PORTABLE
Enjoy the freedom of movement: bring the thermostat around your house whenever you like to promote the temperature.

SAVE
Save up to 30% on your energy bill with the exclusive My Budget function.

CALENDAR
Allows for creation of time periods of the day as you want it.

SMART
Learn your daily habits to optimise energy consumption.

NO CABLES
Wireless thermostat, uses AA batteries.

STATISTICS
Of savings, temperature, and humidity.

GEOLOCATION
Turn the heating system on or off according to the distance you are from your home.

momit
Smart technology for everyonemomit
HOME
THERMOSTATEASY INSTALLATION,
INDEPENDENCE AND SAVINGS

Download the App

You can make all settings for the thermostat to suit your needs and then directly on the App.

Install it

Watch the video and in 30 minutes you'll be enjoying your momit Home Thermostat.

Savings

Start saving up to 30% on your energy bill.

PRODUCT	ORDER CODE	DESCRIPTION
Momit Home Thermostat	MHTWV1	Black
Momit Home Thermostat	MHTWV1	Gold
Momit Home Thermostat	MHTWV1	Silver
Momit Home Thermostat	MHTWV1	Red
Momit Home Thermostat	MHTWV1	Blue