ENDGAME.

RSA ANALYSIS & RECOMMENDATIONS

INTRODUCTION

Over the course of three and half days, there were a variety of findings from the RSA conference with regard to our competitors as well as to RSA and conference booth demos, in general. This document seeks to outline those trends, analyze them and provide recommendations for Endgame products as part of the overall UX strategy.

BACKGROUND

Analysis includes:

- Innovation Sandbox finalists
- North and South hall exhibitors
- 50 companies analyzed spanning more than 50 products
- 116 RSA interface images supplemented with 91 images pulled from online sources

TRENDS

There were several overarching themes and trends at RSA. Not all trends were positive, however, they provide insight into where Endgame can leverage its in-house UX team to create products that are able to overcome these negative trends and differentiate itself in the market.

COLORS

80% of companies (40) utilized dark text on light/white backgrounds which is common practice across most industries. Several companies (5) used exclusively dark backgrounds with light content while several others (5) utilized a mix of dark background with light content that included split screens and dark-with-light on mobile-only content delivery methods. The remaining companies were predominantly white/light background with dark content.

In application development there is no particular "right" solution and of the companies I spoke with who utilized the dark background with light content, they cited doing so for several reasons:
- to differentiate themselves
- to create visuals that "popped" more or had a higher constrast in the data
- to connect to a specific audience type (see Protectwise notes)

Predominant color usage included hues of black/gray, blue and red/orange. The majority of companies chose to utilize shades of blue to denote "safety" or entities that were "good" while reserving use of red and orange to denote things that were "bad" or required further exploration. Black and grays were used for informative/contextual content. The use of yellow, purple and green was minimal and many companies opted for stronger palettes over softer, earth tones.

For Endgame, this means our new color palette speaks to similar industry practices. Of the companies reviewed for this document, approximately 8 (20%) have products that utilize color similar to ours.

GRAPHICAL CONTENT

In terms of application graphic usage, there seemed to be a couple of big trends but generally the use of specific items was scattered and varied not only from company to company but between products and even within products.

BACKGROUND

Dark	Mix
Bright Cloud	Akamai
BT Research	Fortinet
Centripital	Interset
LogRhythm	RSA
ProtectWise	Zimperium

White/Light	
AlertLogic	NowSecure
AT&T	PaloAlto
Bit9/Carbon Black	PeachFuzzer
Caspida	PhireLight-RapidFire
CyberArk	Pixalate
Cybereason	Pradeo TrustReveal
Cylance	ProofPoint
Dell Multicore monitor	PulseSecure
DigitalAttackMap	Qualys
DuoAccessGateway	Rapid7
Fastly	RecordedFuture
FireEye	RiskIQ
Gurucul	SalesForce
Hexis Hawkeye	SilverSky
HP Tipping Point	Splunk
IBM (all products)	Tenable Security Center
Faraday InfoByte	TripWire
Lancope	ZeroFox
Lastline	Zscaler
Level3 Threat map	
Netscope	

COLOR USAGE

Widely used	Sparingly used
Black / Gray	Yellow
Red	Green
Orange	Purple
Blue	

SIMILAR INTERFACE PALETTES

Bright Cloud	Netskope
Cybereason	Rapid7
Gurucul	Splunk (new interface)
Interset	Zerofox

Geographic Maps

The largest trend seen was the use of maps to denote geo-location. Approximately 40% (~18) utilized maps of the world in some fashion. About half of these used maps as the primary interface element for at least one section of their product. Several of these were animated in some fashion to give the feeling of "real-time" or to highlight things changing by the moment.

Network / logical maps

Many companies also utilized standard map libraries for showing entities like network maps with several utilizing libraries contained in the Enterprise product in the "Investigate" and "Advisory Canvas" views.

Charts

The clear winner for charting data was the pie with a vast majority of companies utilizing pie charts within a dashboard view, some utilizing mutiple versions of them even within the same screen.

Other popular charts were line charts for showing trends over time and a reliance, often poorly, on using bar charts. When asked why specific chart types were chosen, most company representatives couldn't explain why. There were a small handfull of companies who were doing truly unique things with their charting/data visualization and they stood out for doing so. Those included **BT Research, Cybereason, Phirelight** and **Protectwise**.

Iconography

Iconography was the most widely overused element for many companies and they tended to rely on its usage to accentuate things often with no real rhyme or reason behind it. Popular use included in the navigation, as helper activities (i.e., search) and as decorative / extraneous. Again, a very small handful of companies used them to define an entity. For example, Cybereason paired a custom icon with their own terminology ("Malop") to define and illustrate their "unique approach".

Product Architecture

The biggest differentiator between "good" products and "great products" after UI was Information Architecture. Many companies, particularly the larger organizations, had products that were not well designed or lacked a clear set of users and user roles to drive their structure. As a result, they came off as confusing, over-generalized or simply bad products.

One problem / story

Companies who focused on one specific problem to solve and could tell a compelling story via their demo seemed to be the clear winners. These were also companies who could state the problem clearly and walk through a potential solution with their product rather than allow a more "exploratory" demo approach.

Single user mode

Many companies, particularly the larger ones (Qualys, RSA) had UI that came off as fragmented, bloated and generally trying to serve too many users. At the RSA booth, I was walked from one monitor to another in order to show me a different part of the app because the sales reps didn't want "the ugly part of the product on this screen". When asked when they would be unifying the disparate sections of the products, I was told "that will never happen - these teams don't have the time to do that".

Another experience involved walking through one product at Qualys whereby the sales rep had to click 7 times to get me from one user role to another, even though the role could potentially have been assigned to the same individual. The architecture was such that the array of products were simply layered on top of each other with nested navigational structures.

In contrast, the more focused products shown by companies like Splunk (new interface) clearly illustrated a problem for which they offered a (seeimingly) simple solution.

Top to Bottom

Products that provided a targeted drilldown approach were very popular, however, few did it well. Many companies attempted to show a dashboard view but then lacked any real way to easily explore a particular area. Often, getting from the dashboard to an area in which the "problem" coud be analyzed and solved required visiting a specific nav item that may have been nested / hidden in order to view more. Few companies were able to seamlessly go from top to bottom back to top to another bottom or problem-solve like an actual user would.

Again, this seemed to be linked to products that did one thing and did it well. This included companies like Zerofox, Zimperium, Splunk (new interface) and for a very large company, Rapid7.

RECOMMENDATIONS

There are several takeaways here for Endgame. This includes both the product itself as well as the demo for the booth in the upcoming trade shows.

At the Show / Demo

LImit the demo script to one or two stories maximum. Keep the stories straightfoward and brief with a very clear problem and a very clear solution. Do not attempt to have the product fix something it cannot do.

Limit the UI to only what is needed to tell the story. Several times I was able to distract from the pitch by simply asking "what does that button/link do?" and interrupt the flow of the sales demo.

Know the product and why it was designed the way it was - be able to speak to why things are grouped together and how that is important to the user. Protectwise was able to explain why the product design was the way it was, offer clear insights into the problems their users face and basically convince me that my guys would want to use the product. That is, they gave me the clear emotional connection to their product.

Create a seamless transaction between the product demo, the booth and the sales rep. In several cases I was "handed off" to another individual when I had specific questions that a sales rep couldn't explain. In some cases, I would get handed off to someone who was already with someone else which left me waiting (and subsequently wandering off.)

Make the schwag align with the product and the problem it's solving (or at least make it meaningful.) Alcohol infused chocolate in a shot glass doesn't actually connect to EDR and the bubbly salesperson could only tell me it was because "everyone likes booze-filled candy!"

Generally I think Endgame showed VERY well in this area. These are more general observations and things to keep in mind for next year and the remaining 2015 shows. The shirts were a hit - I saw several at the Rapid7 party Wednesday night.

In the Product

The new color palette will resonate with users. The key will be in how we use that to differentiate ourselves from the competitors. The best use of a very similar palette was in Splunk's new interface design. It was clean, bold and easy to understand even without a demo.

Chart and data visualization should be familiar. While Protectwise was targeting a very specific audience, their data visualizations were so over-the-top that it was impossible to actually understand. It garnered a ton of buzz for them but it wasn't enough for booth visitors to get on their own. Rapid7, RiskIQ and Zerofox had very clear charts and trend mapping and they were large enough to be seen and understood by the passerbys that may not have been able to actually get a demo.

Limit our focus within the product. This is probably the MOST key area of development for us. While we shouldn't limit what our product can do and for whom, we need to really consider how we structure the product and its various components so that multiple user roles can be established and navigated. Being able to drill down and then resurface ("wander") as a less-experienced individual is very different than being able to go directly to a specific area and perform some action that may be utilized by a more advanced user. However, if our target market spans these two different modes, we need ro ensure our product handles that elegantly. Clear separation of functions for high-level C users from frontline IT should be apparent and thoughtful. Simply forcing every user to start at a C-level dashboard because it's easiest should be avoided. Instead we should explore how we can provide drilldown capabilities that are meaningful for the different users we are targeting.

In the end, I believe we are on the right path. Most companies admitted to either not having UX or outsourcing it to someone not familiar with the company or its products. We have the team inhouse - it's our responsibility to utilize it.