SquareX

Browser Detection and Response (BDR) Whitepaper

sqrx.com

Browser Detection and Response (BDR) Whitepaper

SquareX
INDUSTRY-FIRST
BROWSER DETECTION AND RESPONSE (BDR)™
SECURE EVERY BROWSER, EVERY DEVICE

A. The Evolution of Browsers and Browser Security

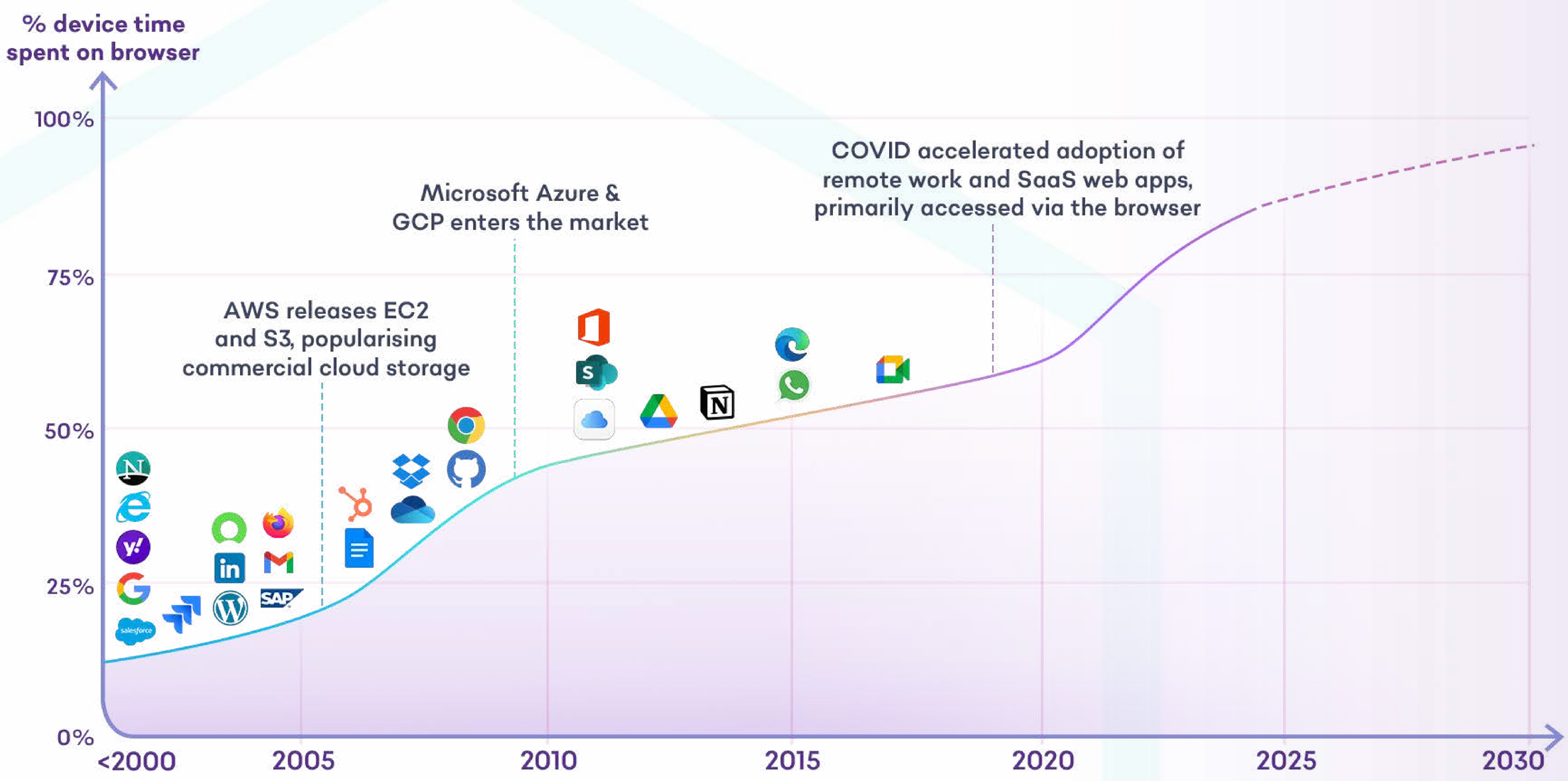
Today, employees spend more than 85% of their productive working hours on the browser. Similarly most company data and resources are accessed through the browser. In other words, browsers are becoming the new endpoint.

Yet, browsers remain one of the least secured applications - most organizations have little visibility into what employees are doing on the browser, and even fewer are able to measure and prevent web attacks. As a result, browsers have become the prime attack vector for adversaries to target employees, which remain to be the weakest link for most organizations.

To understand why there is a mismatch between the role and security of browsers, it is important to delve into the history of the browser itself.

A Brief History of Browsers

Over the past decade, extensions have become significantly more powerful due to advancements in modern web APIs and frontend technologies like HTML, CSS and Javascript. Extensions can now interact with web pages through the Document Object Model (DOM), injecting content scripts to alter how a page looks or behaves. Extensions can also store data locally in the browser, integrate with third-party services and fetch data from multiple apps and sites using browser APIs. As a result, extensions have become a core element in most employees' productivity toolkit, allowing them to be more efficient in everything from scheduling and writing emails to more complex tasks like workflow automation and debugging.



Why is securing the browser especially challenging?

The browser is a complex beast, making it especially challenging to secure. Several reasons for this include:

Heterogeneity
Unlike an app like Salesforce or Microsoft Word where most people perform similar activities in, browsers for a variety of purposes with use cases and workflows that vary significantly between individuals. As a result, it is extremely difficult to create rigid policies that do not impede productivity given the “what” and “how” vary widely.

Mix between Personal and Work
Browsers are one of the few apps which are used for both personal and professional purposes. Even more challenging, users may access the same web apps for both. Common examples include email and file storage sites (e.g. OneDrive, Google Drive). Thus, in addition to security and productivity, security teams now have to think of another trade-off to balance - user privacy. Policies created would have to be identity aware, being able to delineate between personal and work accounts.

Complexity of the Browser
In addition to the proliferation of web apps, the browser itself has also evolved significantly, adding many functionalities to support the different web applications. This includes multiple network protocols, extension subsystems and site permissions. As a result, the attack surface for browsers have also meaningfully expanded.

Zero Visibility
Browsers are often unmanaged. Even in organizations where browsers are managed, most of the control is limited to browser hardening (i.e. enabling/disabling certain features of the browser). Security teams often have limited visibility into user activity within browsers, including how and how often they are targeted by attacks. This lack of insight makes it particularly difficult to analyze the mechanisms of web attacks when a breach occurs. Even more concerning, the majority of web attacks remain entirely undetected, allowing attackers more time to infiltrate the organization.

How do existing tools fare when it comes to protecting against web attacks?

For a detailed feature comparison, refer to our Buyer's Guide in Appendix A-C.

Chrome Enterprise

Browser vendors like Chrome typically focus on two things - (i) patching the browsers and (ii) browser hardening. The latter is provided on enterprise versions of the browsers, such as Chrome Enterprise Premium, and essentially allows admins to enable and disable certain features within the browser (e.g. blacklist site categories, extensions). However, these rules are static and do not provide any real time detection and mitigation of web attacks.

Enterprise Browsers

In the past 4 years, several enterprise browsers such as Island and Talon have emerged. However, enterprise browsers are primarily focused on access management control and have limited capabilities when it comes to detecting and preventing web attacks. Additionally, the cost and change management required to migrate all employees into a new browser is prohibitive to most organizations.

EDRs

EDRs primarily focus on inspecting files and processes at the endpoint and have no visibility into the browser. In other words, detection only begins when a malicious file is downloaded. Unfortunately, many web attacks today live and die in the browser including phishing, identity attacks and data exfiltration that never triggers a file download.

SASE/SSE

Most organizations rely on Secure Web Gateways (SWGs) as part of the SASE/SSE suite to detect and mitigate web attacks. They primarily rely on SSL interception to determine if a domain is malicious. Most of these solutions were invented between 10 to 15 years ago, back when web applications were relatively simpler, allowing these tools to infer what is happening in the browser from the network layer by inspecting HTML, CSS and Javascript.

However, due to the complex nature of browsers and web apps today, it is impossible to accurately do such inference without having direct access to browser metrics such as DOM changes, user interaction, site permissions, clipboard content and tab/window context.

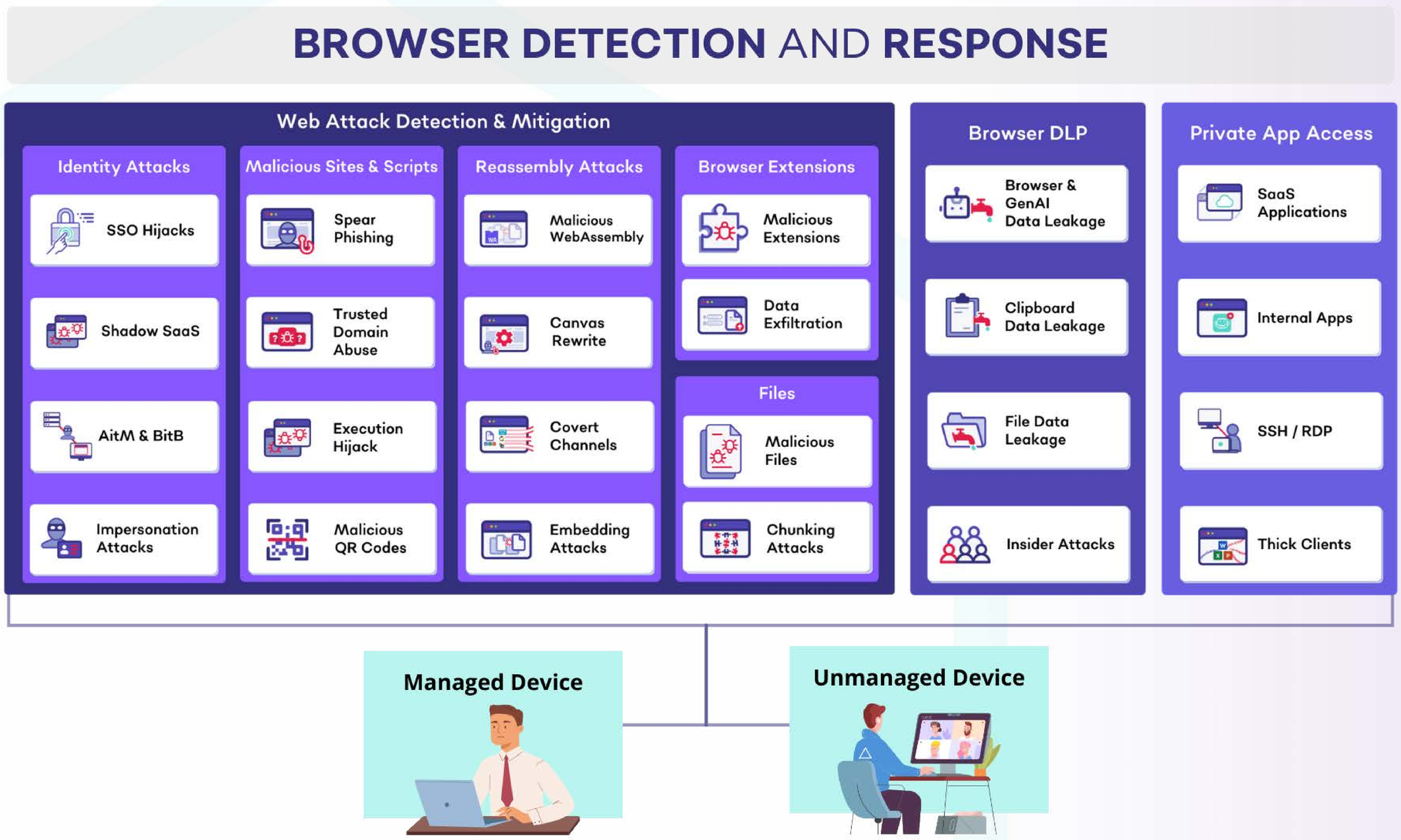
SquareX revealed 25 attacks that exploit these architectural limitations at DEF CON 32, showing a complete bypass of all major SASE/SSE vendors. To test your SASE/SSE solution against these attacks, use this free Web Security Posture Assessment tool. These are just one of many attack classes that have successfully bypassed SWGs, as evident in the Okta Breach and Qilin Ransomware Attacks earlier this year. Our security research team has compiled 90+ such attacks reported in the news.

B. Browser Detection and Response (BDR)

As the future of work is evolving, security must evolve alongside it too. There are three components that are critical to secure a primarily browser-based work environment:

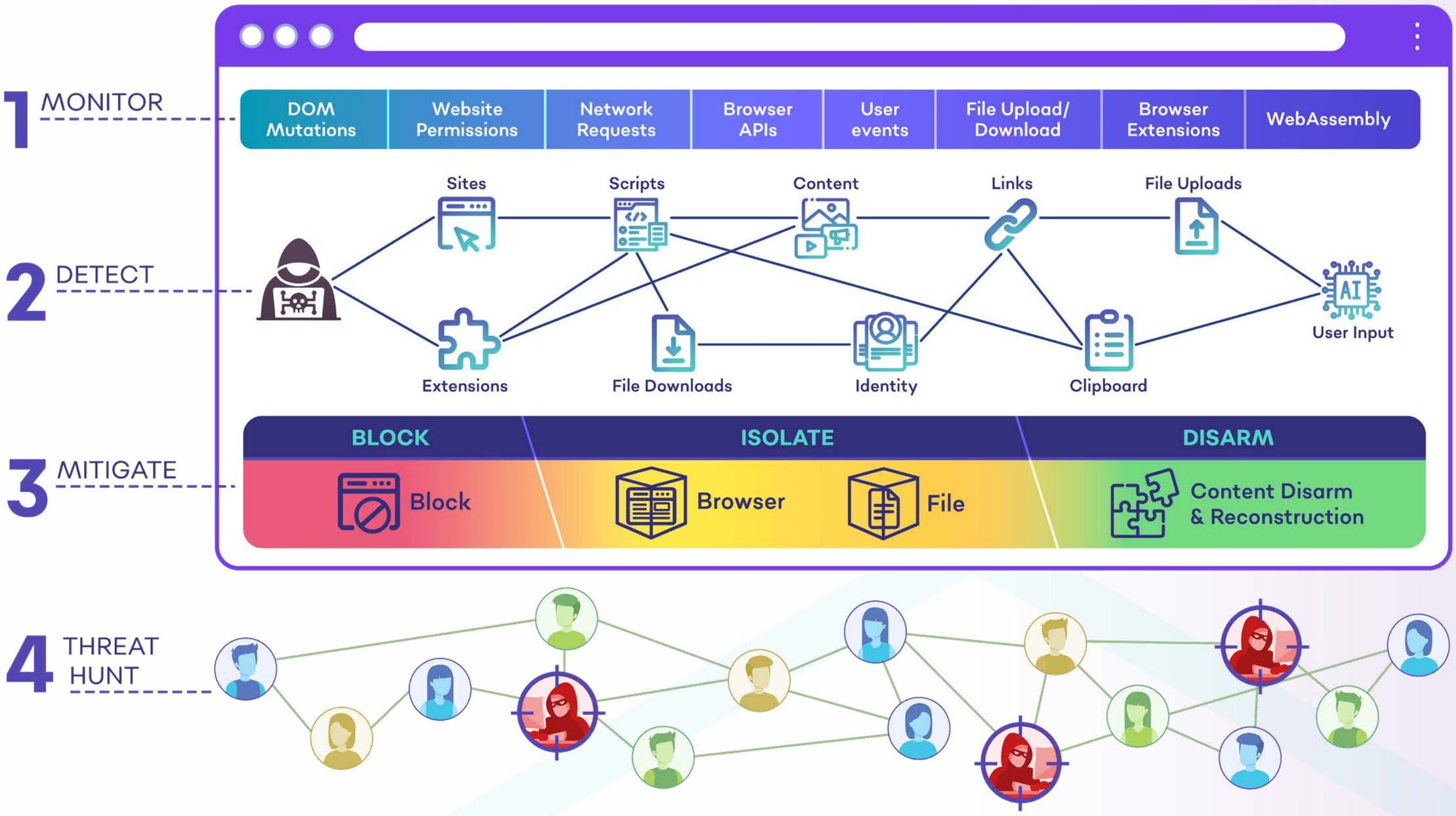
- **Web Threat Detection & Mitigation** including identity attacks, malicious sites & scripts, malicious browser extensions and malicious files
- **Browser DLP** including genAI DLP, clipboard DLP, file DLP and insider attacks
- **Private App Access** to provide secure access to web applications and private apps via the browser, including for BYOD/unmanaged devices

This whitepaper will primarily focus on the first two components. To learn more about our private app access solution, access our VDI Replacement Solution Guide.



What is a BDR?

SquareX's industry-first Browser Detection and Response (BDR) solution detects, mitigates and threat-hunt client-side web attacks targeting employees in real time. The solution comes in the form of a lightweight browser extension that can be deployed to existing browsers via a simple group policy.



There are four components to the BDR:

Monitor

As a browser-native solution, SquareX has access to rich browser metrics including DOM mutation, website permissions, network requests and browser APIs. SquareX is able to track all file upload/download, clipboard content and browser extension activities to identify malicious activity and prevent data loss.

Detect

With the browser metrics above, SquareX can detect any malicious activity happening in the browser. The five most common vector of attacks are:

1. **Sites -** malicious sites can deceive users to divulge credentials/sensitive information or execute code (e.g. drive-by downloads). In addition to URL filtering, SquareX performs real time analysis of user-browser interaction, content inspection and DOM changes to detect and block threats before users are compromised. This allows SquareX to capture advanced attacks such as Browser-in-the Browser (BiTB), Captcha-walled, Multi-hop and over 90 other web attacks discovered to date that cannot be detected by SWGs.

2. **Files -** SquareX's industry-first client-side file scanner allows the BDR to intercept and scan every file before a download is triggered. This allows malicious payloads/content to be detected in the browser itself, without sending the file to an external server. In addition to being more privacy safe, this allows SquareX to scan files up to 50 times larger than SWGs can. Conversely, SquareX also inspects all file uploads for PII and other sensitive information for data loss prevention, including preventing upload of company files to personal email and/or file storage accounts.

3. **Extensions -** malicious or compromised extensions can exfiltrate data, inject malicious scripts, or serve as a bridgehead for further attacks. As most security teams manage extensions through one-off whitelisting, attackers frequently purchase or hack into popular extensions, turning benign extensions already installed in millions of browsers into malicious ones without security teams noticing. SquareX inspect these changes in extension behaviour and permissions live, automatically blocking any suspicious activities coming from installed extensions in real time.

4. **Identity -** SquareX allows enterprises to create granular policies on the SaaS apps and authentication methods each user can use. This prevents employees from accessing unauthorized and shadow SaaS applications, as well as those that mimic enterprise login pages. Additionally, security teams can enforce password best practices such as implementing password strength requirements across all sites and preventing password re-use across sites.

5. **Clipboard -** inspection of clipboard content to prevent copy-pasting of sensitive information to prevent data loss. Policies can also be enforced on specific sites such as blocking paste to GenAI sites or blocking copy from enterprise web apps.

SquareX Threat Detection Library

SquareX closely monitors all major threat feeds to maintain a threat detection library, containing policies that defend against the latest threats and threat actors. This policy library is updated live on a daily basis, automatically pushing new policies to all end users, stopping novel attacks directly in the browser.

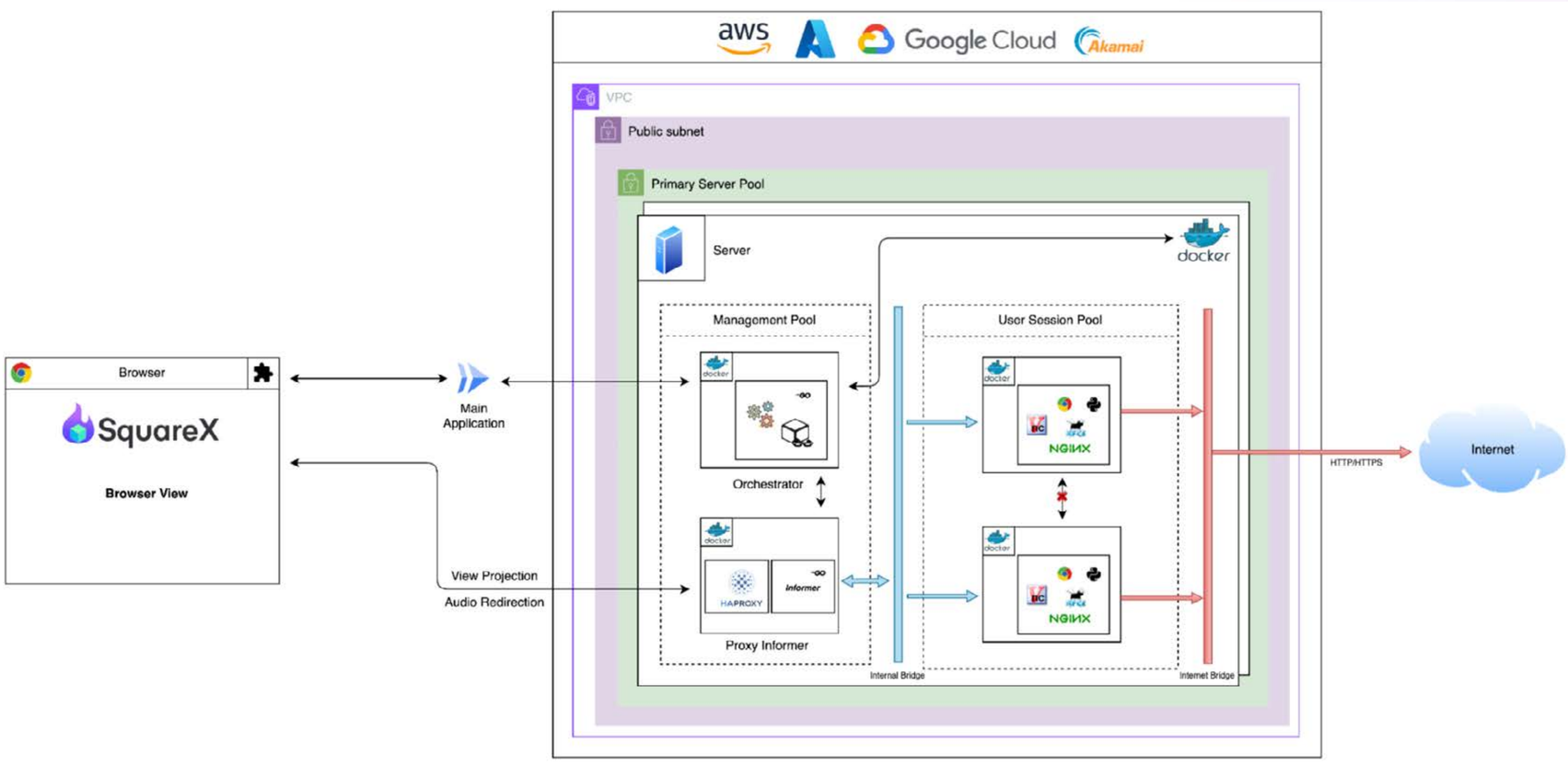
From an admin perspective, the library abstracts away the need for security teams to figure out a mitigation policy whenever a new attack is discovered. Additionally, admins will have full visibility on whether their organization is vulnerable to these attacks, either by the identified adversaries or other attackers using a similar technique.

Mitigate

In addition to allow and block, SquareX provides several additional mitigation actions whenever malicious activity is detected, enabling employees to continue working in a safe environment:

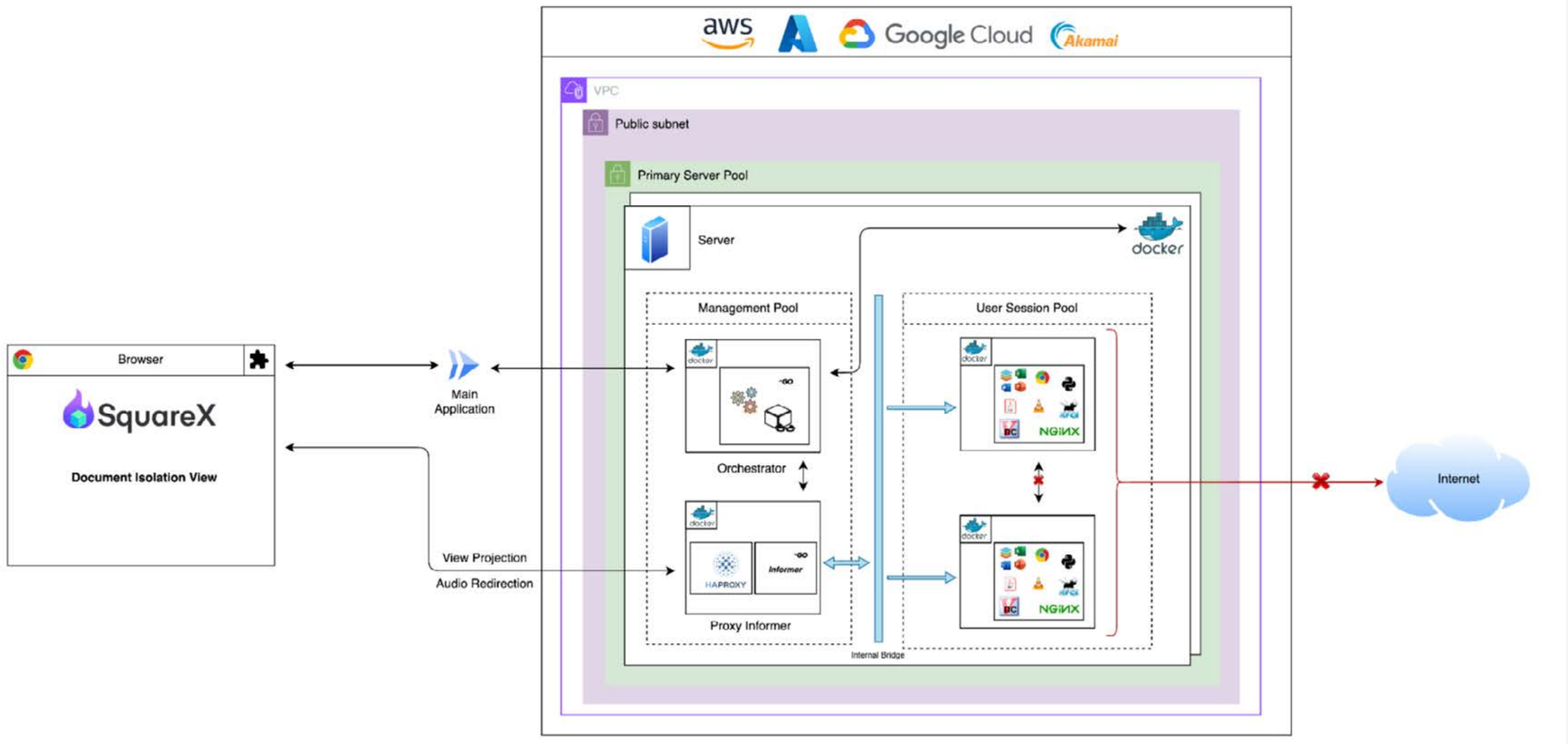
Browser Isolation

Enterprises can set policies to automatically open suspicious sites in an isolated sandbox. This feature can be especially useful for individuals that travel frequently, such as sales teams, and require secure, disposable browsing sessions while they are on the road. Additionally, security teams may also use these disposable browsers to inspect malicious sites.



File Isolation

Employees can open up malicious files in a safe, disposable file viewer (DFV) isolated from the endpoint where they can open, edit and collaborate on the file without compromising the device. Similar to the disposable browser, DFVs can also be used by security teams to detonate malicious files in a safe manner.



Content Disarm and Reconstruction (CDR)

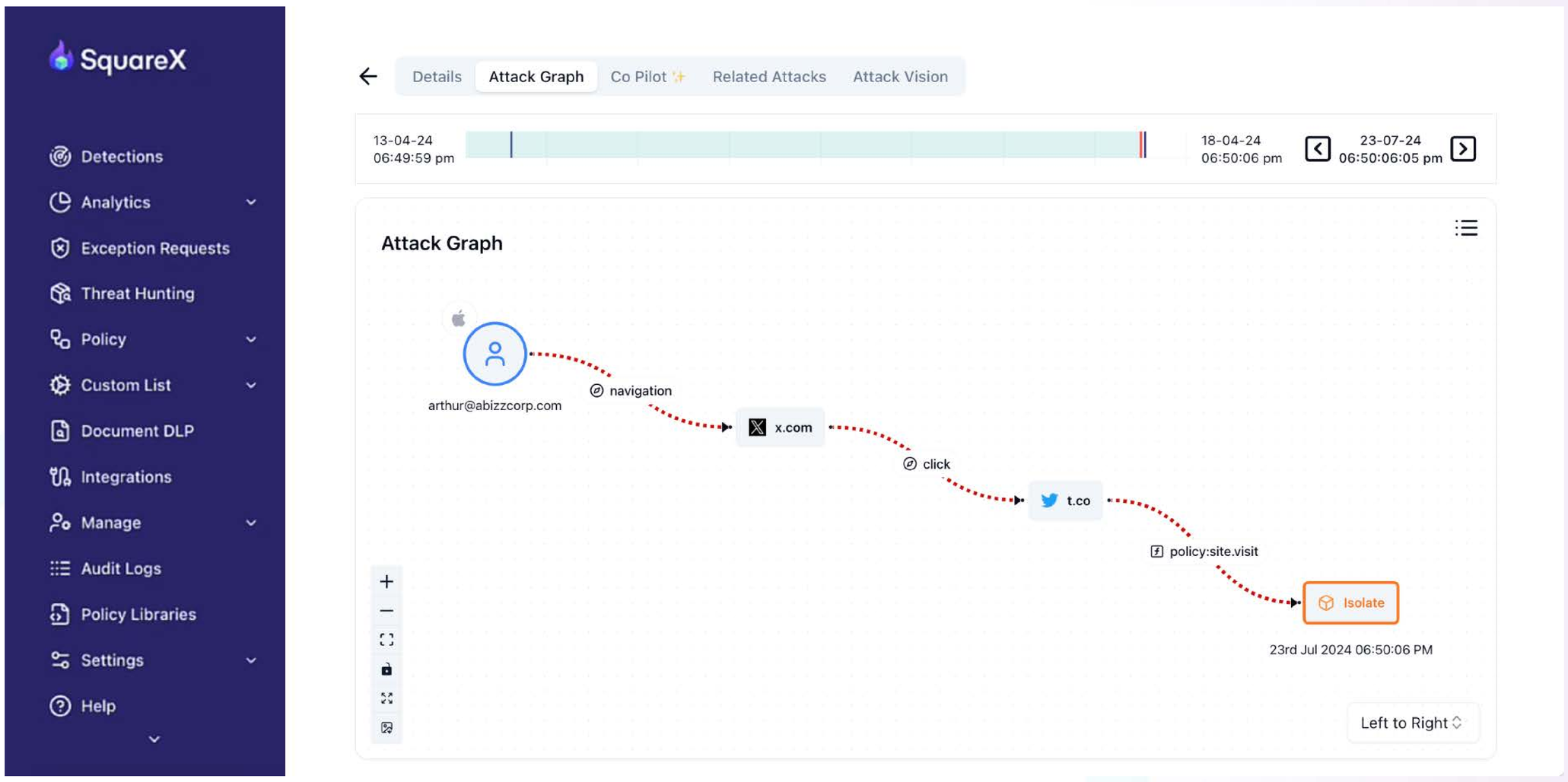
Where employees need to download files containing malicious macros, SquareX can perform CDR to remove any malicious macros, providing the user with a safe, cleaned-up file.

Threat Hunt

SquareX leverages various rich browser metrics to provide a detailed and comprehensive view on attack mechanisms, enabling security teams to have granular visibility on how adversaries are attacking employees in the browser. Some key features include:

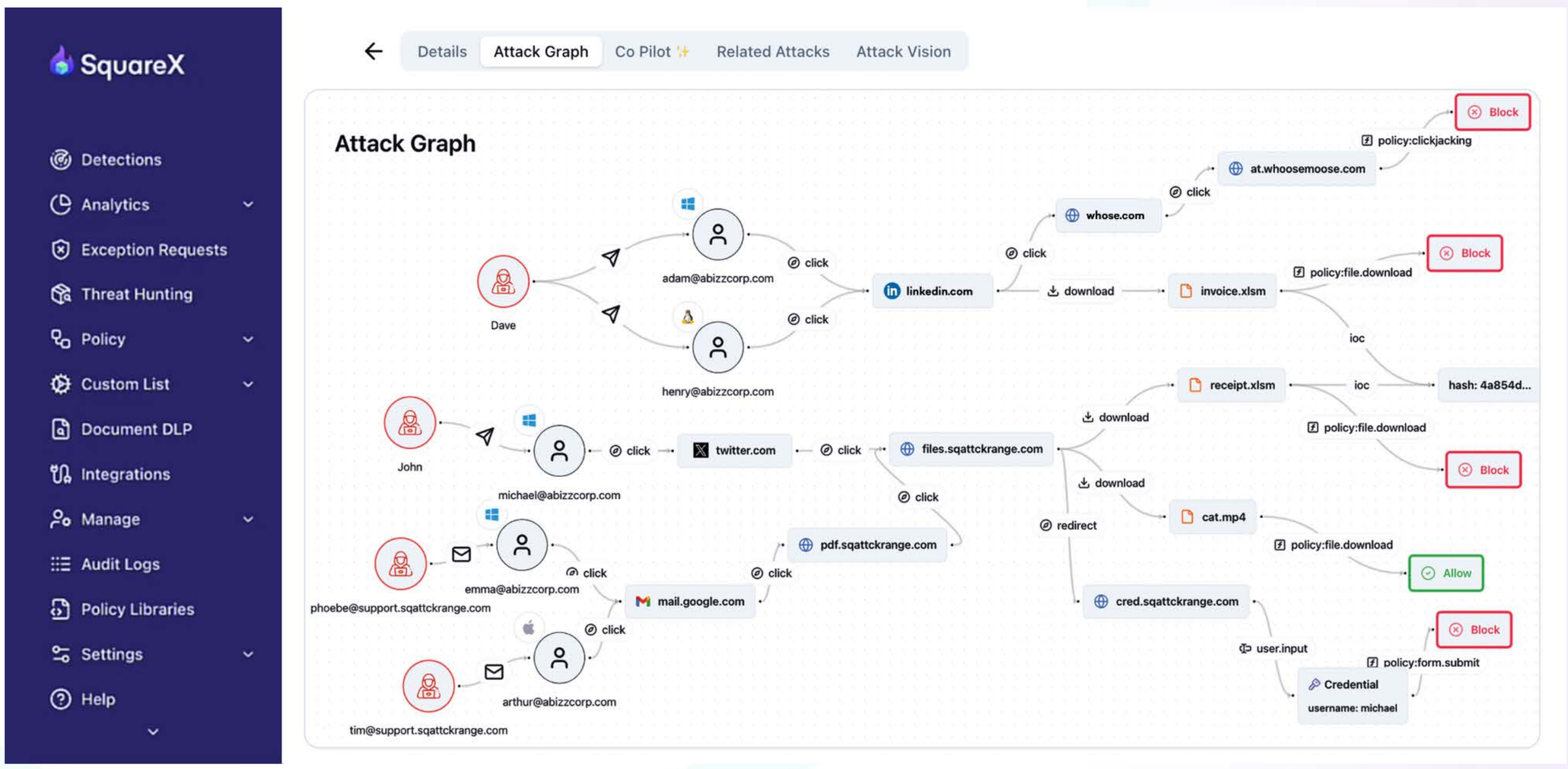
Attack Graph

SquareX's detailed attack graph lays out the different sites and actions users took before the policy is triggered, allowing security teams to understand in detail the attack path that adversaries are using to target employees.



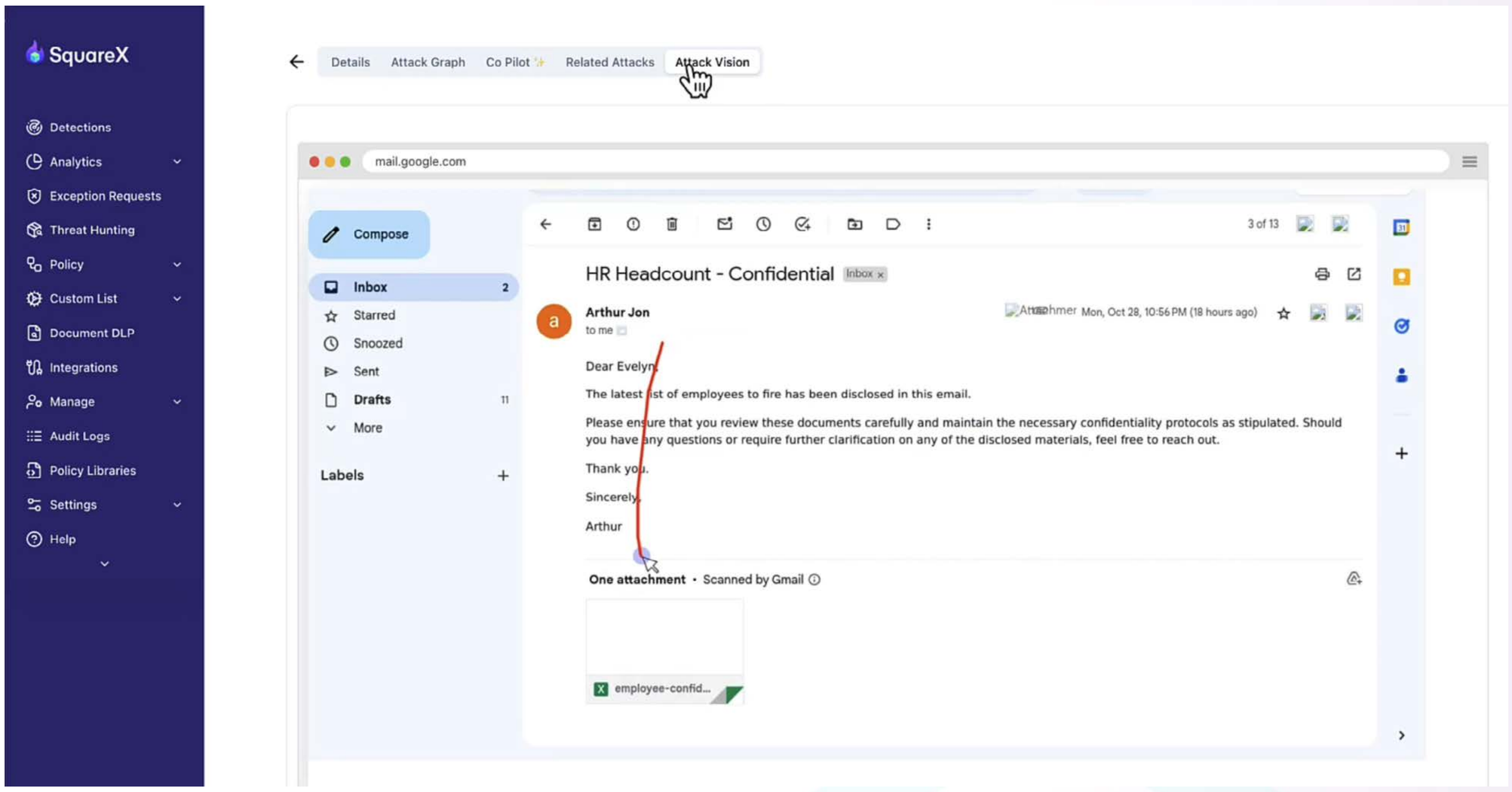
Attack Correlation

Often, attack campaigns will target multiple users in the same organization. The same attacker may run multiple campaigns simultaneously. SquareX is able to correlate all such attacks enterprise-wide to understand who and how different employee groups are being attacked to perform root cause analysis.



Attack Vision

For vulnerable user groups, such as potential insider threats, security teams can turn on a feature called attack vision. With DOM reconstruction, admins can simulate the exact user view and activities they are performing in the last 30 seconds leading up to the policy hit. This helps security teams get a definitive view on whether a breach is due to negligence or malicious intent.



Acquire Artefact

Similarly, security teams have the option to acquire a copy of any malicious files detected. In addition to a detailed analysis of detected malicious macros that come as a default, this allows admins to detonate these malicious files in our disposable file viewer.

Co-pilot

SquareX's co-pilot automatically generates a custom report for each attack, detailing in prose what happened, who is affected within the organization and suggested remediation actions.

FAQ: Data Security & Privacy

What information gets sent to SquareX?

SquareX was built with data privacy as a priority. As a client side solution, minimal data gets sent to SquareX's servers. For example, unlike existing server side solutions (e.g. SWGs), our browser-native file scanner does not require any file to be sent to SquareX's servers for malware analysis. When a policy hits, the only information SquareX's threat hunting capabilities require is high level identifiers (e.g. file name, website URL, user ID). No files, content or sensitive information is collected unless admins turn on advanced monitoring features like Acquire Artefact or Attack Vision, which can be selectively turned on for specific policies or vulnerable user groups.

How is AI used in SquareX? Is customer data being used to train SquareX's model?

SquareX uses AI in two ways. First, our AI policy engine helps select the right parameters based on the business case admins put in using natural language. Second, our co-pilot summarizes attack graphs to generate reports and suggest remediation policies. In other words, SquareX purely uses AI for summarization and assisting parameter selection within the admin panel, therefore zero customer data is used to train our models.

Conclusion

As browsers are slowly becoming the primary way in which security and productivity is being delivered within organizations, this whitepaper is a call to action for enterprises to take a more proactive strategy when it comes to browser security. Due to the speed at which the volume and complexity of web attacks is evolving, the traditional “whack-a-mole” approach is proving to be a losing game. It is imperative for organizations to think like an attacker and block attack mechanisms instead of individual malicious domains and the only way to do this is to have a BDR tool that has complete visibility and control over all activities performed in the browser.

FAQ: Deploying SquareX

How is SquareX’s BDR deployed?
SquareX’s BDR comes in the form of a lightweight browser extension that can be deployed via group policies through device management solutions like Microsoft Intune and Jamf. Once installed, end users will not be able to disable SquareX even if they have administrator privileges.

The benefit of deploying as an extension is that there is no need to install and migrate users to separate enterprise browsers. Employees can keep their existing browsers and workflows, minimizing the change management required.

Which browsers is SquareX compatible with?
SquareX is compatible with all major browsers including Chrome, Edge, Safari, Firefox and all other Chromium-based browsers.

Does SquareX work on unmanaged/BYOD devices?
Yes, SquareX can also secure browsers on unmanaged devices. In fact, many customers use SquareX to secure 3rd party contractors and BYOD devices where they have limited control over today. In this case, SquareX works as a 3rd-party MFA to the customer’s IDP solution, preventing users from accessing any company resources when SquareX is not running.

How much work is involved in setting up SquareX policies?
SquareX comes with a policy library of best practice policies, which is continuously updated as our research teams uncover more attacks. However, if your security team requires additional and/or modified policies, SquareX’s AI policy engine allows admins to automatically select the right parameters by simply typing in the business case in natural language (e.g. “Isolate all files containing malicious macros”). These policies are highly granular, and can be applied to specific user groups as required.

What integrations does SquareX have with existing security tools?
SquareX integrates with multiple tools in the security stack to provide flexibility and convenience for security teams. The two integrations to highlight are:

- **IDP -** admins can import existing users and user groups from the IDP, allowing them to apply policies to specific user groups. If preferred, these user groups can also be generated directly on our platform
- **SIEM -** SquareX is integrated with most major SIEMs and can send live detection data for monitoring through the SIEM

Is SquareX MV3 compliant?
Yes, SquareX is built in accordance with the Manifest V3 guidelines from inception. Hence, all functionalities will work under MV3.

Appendix

Appendix A. BDR vs. Chrome Enterprise Premium

	Chrome Enterprise Premium	BDR
Deployment/ Installation	• Managed Chrome Browser • Chrome only	• Easily deployed as agentless browser extension via managed browsers or MDM • Browser agnostic
SaaS Access	• Context-aware access to SaaS, Google Cloud and web apps	• Context-aware access to SaaS & web apps
User action control	• Limited to Google web applications • Limited ability to control user actions, typically work by black/whitelisting entire sites	• Insight into all web apps • Granular control over site-specific user actions (e.g. user input, clipboard copy/paste, file upload and download)
Threat Protection	• Protect against known malware and phishing sites • Static category-based web filtering • Malware and phishing only	• Heuristic analysis to protect against zero day attacks • Real-time inspection of individual sites & files • Full protection against web-based threats encompassing malicious websites, files, scripts, and networks.
Data Leakage Prevention	• Basic regex and string checks	• Advanced DLP ML models incl. advanced regex, content inspection, file inspection & GenAI DLP
Access Controls	• Identity context only on Google Apps • No access control for internal apps	• Identity context on all web apps • Access control for all web and internal apps via RDP, SSH and thick clients
User Activity Logs	• Google Drive activity only	• Full visibility to user activity on any web app upon policy trigger
Isolation	• No Remote Browser Isolation options	• Web-based browser and file isolation

Appendix B. Buyer's Guide - BDR vs. Enterprise Browsers

	Subcategory	BDR	Enterprise Browsers
Monitor	Network Requests, File Download / Upload Events on the Network	✓	✓
	DOM Mutations, Website Permissions, Browser APIs, User Events, Browser Extensions, WebAssembly, Clipboard	✓	✗
Detect	Comprehensive Attack Detection	90+ unique attacks	Basic Detections
	In-browser File Analyzer: File-based Malware Analysis, Office Document Analysis Engine	✓	✗
	In-browser File DLP: Semantic Document Similarity Checks	✓	✗
	Identity Attacks: OAuth, SAML-based Authentication Checks and Controls	✓	✗
	QR Code Detect-Mitigation	✓	✗
	WASM analysis	✓	✗
	Last Mile Reassembly	✓	✗
Mitigate	Remote Browser Isolation	✓	✗
	Remote Document Isolation	✓	✗
	Content Disarm & Reconstruction	✓	✗
Threat Hunt	Detailed Attack Graphs	✓	✗
	Incident Recording (Attack Vision)	✓	✗
	Enterprise-Wide Attack Correlation	✓	✗
	Incident Reports (Co pilot summary)	✓	✗
	Artefact Collection (File, Clipboard...)	✓	✗

Appendix C. Buyer's Guide - BDR vs. SWG vs. EDR

	Subcategory	BDR	SWG	EDR
Monitor	Network Requests, File Download / Upload Events on the Network	✓	✓	✓
	DOM Mutations, Website Permissions, Browser APIs, User Events, Browser Extensions, WebAssembly, Clipboard	✓	✗	✗
Detect	Comprehensive Web Attack Detection	90+ unique attacks	Limited	✗
	Identity Context Aware DLP	✓	✗	✗
	SaaS App Context Aware DLP	✓	✗	✗
	In-browser File Analyzer: File-based Malware Analysis, Office Document Analysis Engine	✓	✗	✗
	In-browser File DLP: Semantic Document Similarity Checks	✓	✗	✗
	Identity Context Aware DLP	✓	✗	✓
	Identity Attacks: OAuth, SAML-based Authentication Checks and Controls	✓	✗	✗
	QR Code Detect-Mitigation	✓	✗	✗
	WASM analysis	✓	✗	✗
	Last Mile Reassembly	✓	✗	✗
Mitigate	Remote Browser Isolation	✓	Add-on	✗
	Remote Document Isolation	✓	Add-on, partial implementation	✗
	Content Disarm & Reconstruction	✓	✓	✗
Threat Hunt	Detailed Attack Graphs	✓	✗	✗
	Incident Recording (Attack Vision)	✓	✗	✗
	Enterprise-Wide Attack Correlation	✓	✗	✗
	Incident Reports (Co pilot summary)	✓	✗	✗
	Artefact Collection (File, Clipboard...)	✓	✗	✗

SquareX

INDUSTRY-FIRST

BROWSER DETECTION AND RESPONSE (BDR)™

SECURE EVERY BROWSER, EVERY DEVICE

Contact us here to learn more about SquareX's BDR solution