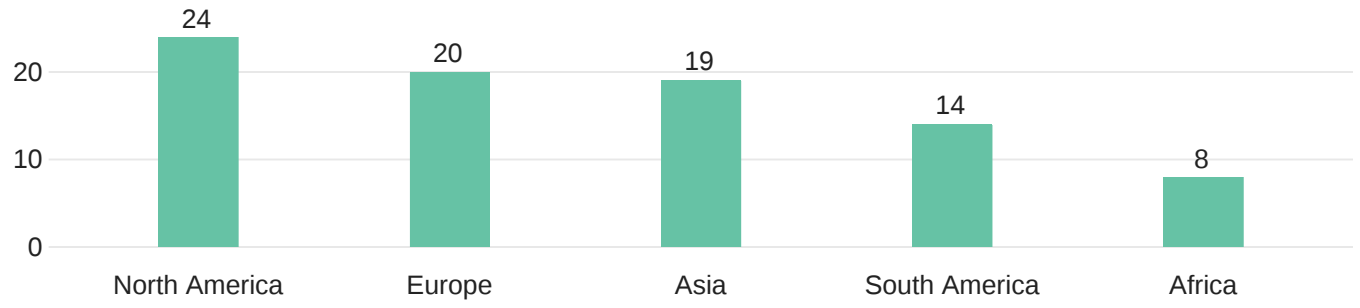
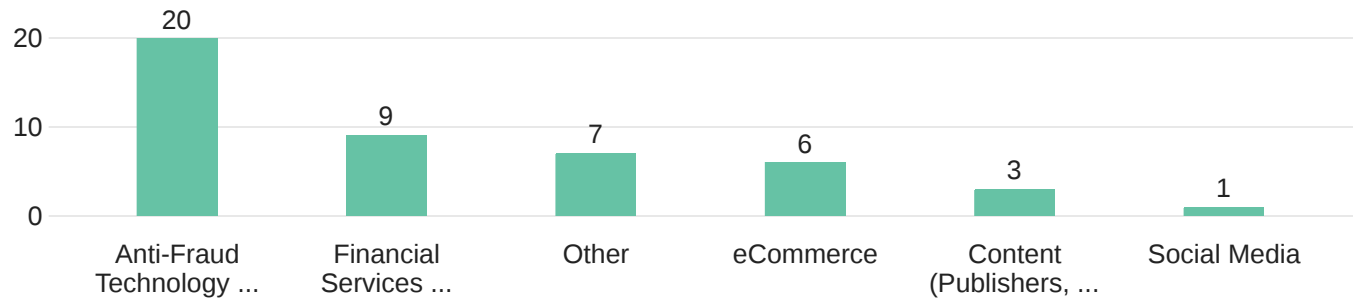
Company Operating Region

30 Responses



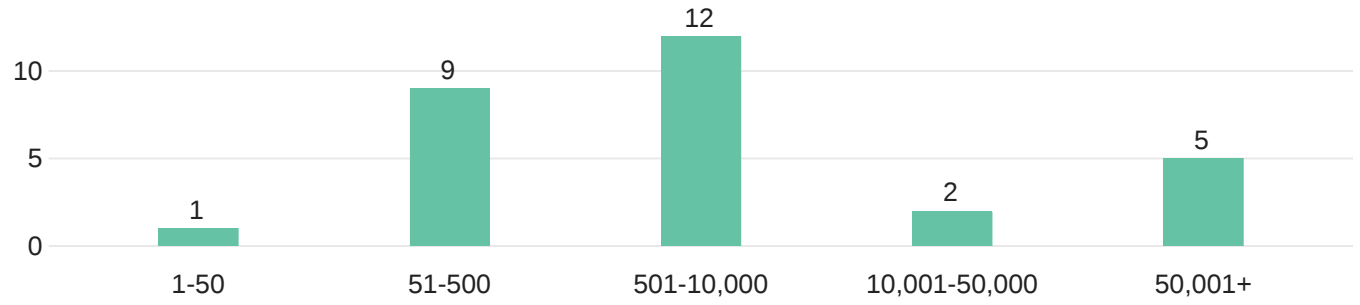
Company Industry

30 Responses

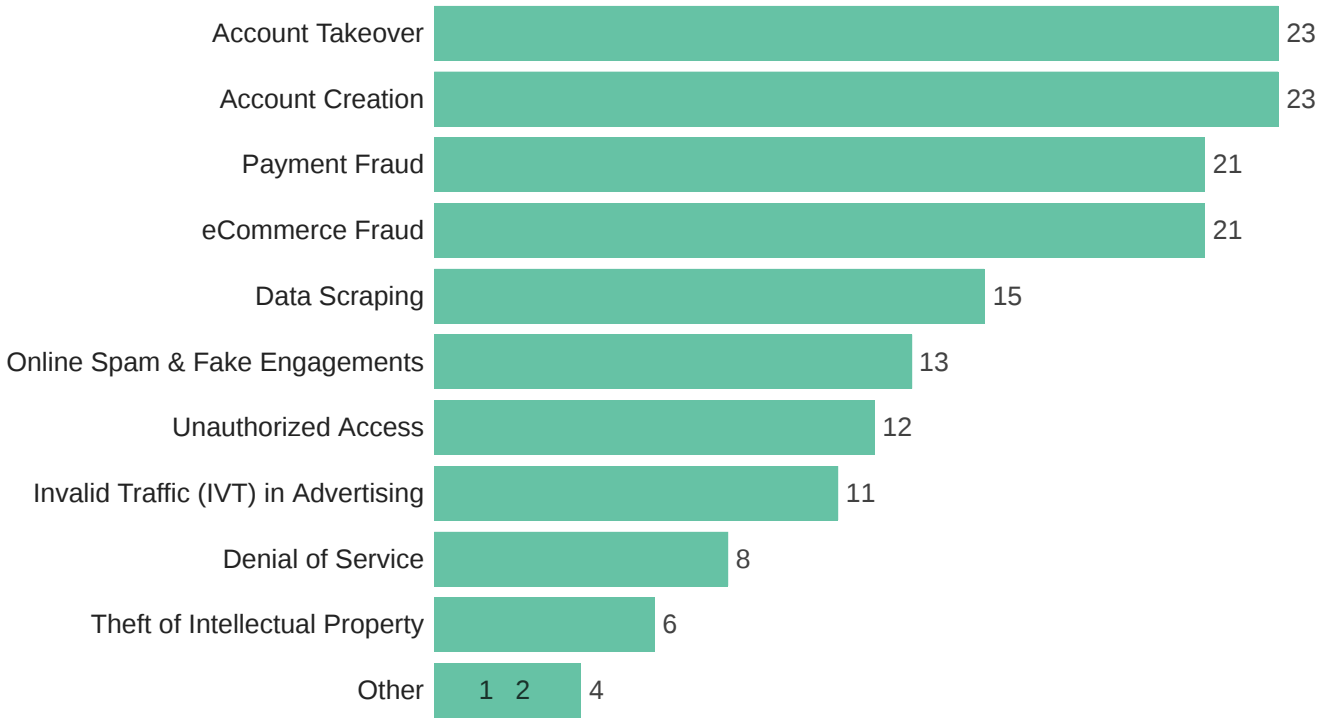


Company Size (number of employees)

30 Responses



Which use cases are applicable to your organization?



Other use cases (free text answers)

Financial Transactions

Login

Fraudulent activity using the platform

Malicious Download Compromised Landing Site/Pages

Payments

Browser compromise Auto-Redirect

Scam Ads Cryptojacking

Rank the use cases in order of importance

Note that a lower mean indicates higher importance

Field	Mean
Invalid Traffic (IVT) in Advertising	2.55
Payment Fraud	2.90
Account Takeover	2.91
Account Creation	2.96
eCommerce Fraud	3.24
Data Scraping	5.00
Online Spam & Fake Engagements	5.08
Unauthorized Access	5.75
Denial of Service	6.13
Theft of Intellectual Property	8.17

Across ALL use cases, the most selected capabilities

Note that all use cases had the same set of capabilities that respondents could choose from. Once a respondent selected a use case as being applicable to their organization, they were then asked to select the capabilities that were important for that particular use case.

Field	Total
Geo Attestation: Confirm the geographic location of a specific device	116
Counters: Ability to keep an approximate count of how often a physical device has done a specific action.	106
Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device	103
Recognize whether the same device is seen again in the context of multiple identities (e.g., Seeing many different identities' data coming from the same device can be indicative of account take over)	95
Device and Boot attestation: Confirm that the device and OS matches the reported model and version	88
User Presence: Confirm that a user is present	84
Intent: Reason about the degree of coordination among an arbitrary set of users	58
App/Site attestation: Confirm that the application or website on the device match the application or website reported to the service	56
Post-boot attestation: Check for up-to-date security patches and known strains of malware	47
Element Visibility: Confirm that a given visual element actually activated pixels on the device	39
Other	25
Other	14

For the 'Account Creation' use case, select all relevant capabilities and add ones not listed below

Field	Choice Count
Geo Attestation: Confirm the geographic location of a specific device	20
Recognize whether the same device is seen again in the context of multiple identities: For example, seeing many different identities' data coming from the same device can be indicative of account take over	19
User Presence: Confirm that a user is present	18
Counters: Ability to keep an approximate count of how often a physical device has done a specific action	17
Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device	17
Device and Boot attestation: Confirm that the device and OS matches the reported model and version	16
App/Site attestation: Confirm that the application or website on the device matches the application or website reported to the service	12
Intent: Reason about the degree of coordination among an arbitrary set of users	11
Post-boot attestation: Check for up-to-date security patches and known strains of malware	11
Element Visibility: Confirm that a given visual element actually activated pixels on the device	7
Other	6
Other	3

Other Capabilities (free text answers)

1. Unique Identifier: Provide ability to uniquely identify and track users across the industry.

Detect automatic account creation

Device fingerprinting/inspection to determine if a device is typical of an active fraud ring

Identity Verification

Whether the device is being controlled by automation software

a way to technologically enforce a "1 per person" limit

2. Campaign Binding: With user consent, bind a credential (such as a cookie) to a campaign and or image to ensure it is not compromised at any stage after scanning.

Inspect device IP and compare to IP ranges of known bad actors, or VPN/proxy services

Whether the browser has been modified in some way

For the 'Account Creation' use case, rank capabilities in order of importance

Note that a lower mean indicates higher importance

Field	Mean
Recognize whether the same device is seen again in the context of multiple identities: For example, seeing many different identities' data coming from the same device can be indicative of account take over	2.89
Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device	2.94
Counters: Ability to keep an approximate count of how often a physical device has done a specific action	3.47
Geo Attestation: Confirm the geographic location of a specific device	4.53
Device and Boot attestation: Confirm that the device and OS matches the reported model and version	5.50
User Presence: Confirm that a user is present	5.76
App/Site attestation: Confirm that the application or website on the device matches the application or website reported to the service	6.00
Post-boot attestation: Check for up-to-date security patches and known strains of malware	6.91
Intent: Reason about the degree of coordination among an arbitrary set of users	7.18
Element Visibility: Confirm that a given visual element actually activated pixels on the device	7.83
Other	1.17
Other	2.33

For the 'Payment Fraud' use case, select all relevant capabilities and add ones not listed below

Field	Choice Count
Recognize whether the same device is seen again in the context of multiple identities: For example, seeing many different identities' data coming from the same device can be indicative of account take over	17
Geo Attestation: Confirm the geographic location of a specific device	17
Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device	15
Counters: Ability to keep an approximate count of how often a physical device has done a specific action	14
User Presence: Confirm that a user is present	12
Device and Boot attestation: Confirm that the device and OS matches the reported model and version	12
Post-boot attestation: Check for up-to-date security patches and known strains of malware	7
App/Site attestation: Confirm that the application or website on the device match the application or website reported to the service	6
Intent: Reason about the degree of coordination among an arbitrary set of users	6
Element Visibility: Confirm that a given visual element actually activated pixels on the device	5
Other	4
Other	2

Other Capabilities (free text answers)

Identity Verification
a way to technologically enforce a "1 per person" limit
Inspect device IP and compare to IP ranges of known bad actors, or VPN/proxy services
Whether the device is being controlled by automation software
Device fingerprinting/inspection to determine if a device is typical of an active fraud ring
Whether the browser has been modified in some way

For the 'Payment Fraud' use case, rank capabilities in order of importance

Note that a lower mean indicates higher importance

Field	Mean
Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device	2.00
Counters: Ability to keep an approximate count of how often a physical device has done a specific action	2.69
Recognize whether the same device is seen again in the context of multiple identities: For example, seeing many different identities' data coming from the same device can be indicative of account take over	3.21
Geo Attestation: Confirm the geographic location of a specific device	4.40
User Presence: Confirm that a user is present	5.25
Device and Boot attestation: Confirm that the device and OS matches the reported model and version	5.30
Intent: Reason about the degree of coordination among an arbitrary set of users	6.50
App/Site attestation: Confirm that the application or website on the device match the application or website reported to the service	6.60
Post-boot attestation: Check for up-to-date security patches and known strains of malware	7.14
Element Visibility: Confirm that a given visual element actually activated pixels on the device	7.60
Other	1.50
Other	3.00

For the 'eCommerce Fraud' use case, select all relevant capabilities add ones not listed below

Field	Choice Count
Geo Attestation: Confirm the geographic location of a specific device	18
Recognize whether the same device is seen again in the context of multiple identities: For example, seeing many different identities' data coming from the same device can be indicative of account take over	16
Counters: Ability to keep an approximate count of how often a physical device has done a specific action	16
Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device	15
Device and Boot attestation: Confirm that the device and OS matches the reported model and version	12
User Presence: Confirm that a user is present	10
Post-boot attestation: Check for up-to-date security patches and known strains of malware	8
App/Site attestation: Confirm that the application or website on the device match the application or website reported to the service	7
Intent: Reason about the degree of coordination among an arbitrary set of users	6
Element Visibility: Confirm that a given visual element actually activated pixels on the device	4
Other	4
Other	2

Other Capabilities (free text answers)

Identity Verification
a way to technologically enforce a "1 per person" limit
Device fingerprinting/inspection to determine if a device is typical of an active fraud ring
Whether the device is being controlled by automation software
Inspect device IP and compare to IP ranges of known bad actors, or VPN/proxy services
Whether the browser has been modified in some way

For the 'eCommerce Fraud' use case, rank capabilities in order of importance

Note that a lower mean indicates higher importance

Field	Mean
Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device	2.58
Counters: Ability to keep an approximate count of how often a physical device has done a specific action	2.64
Recognize whether the same device is seen again in the context of multiple identities: For example, seeing many different identities' data coming from the same device can be indicative of account take over	3.08
Geo Attestation: Confirm the geographic location of a specific device	4.36
Device and Boot attestation: Confirm that the device and OS matches the reported model and version	5.18
User Presence: Confirm that a user is present	5.33
Intent: Reason about the degree of coordination among an arbitrary set of users	5.83
App/Site attestation: Confirm that the application or website on the device match the application or website reported to the service	6.17
Element Visibility: Confirm that a given visual element actually activated pixels on the device	6.75
Post-boot attestation: Check for up-to-date security patches and known strains of malware	7.88
Other	1.75
Other	2.50

For the 'Account Takeover' use case, select all relevant capabilities and add ones not listed below

Field	Choice Count
Recognize whether the same device is seen again in the context of multiple identities: For example, seeing many different identities' data coming from the same device can be indicative of account take over	19
Geo Attestation: Confirm the geographic location of a specific device	18
Counters: Ability to keep an approximate count of how often a physical device has done a specific action.	17
Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device	17
Device and Boot attestation: Confirm that the device and OS matches the reported model and version	15
User Presence: Confirm that a user is present	13
Intent: Reason about the degree of coordination among an arbitrary set of users	8
App/Site attestation: Confirm that the application or website on the device match the application or website reported to the service	7
Element Visibility: Confirm that a given visual element actually activated pixels on the device	6
Post-boot attestation: Check for up-to-date security patches and known strains of malware	6
Other	5
Other	2

Other capabilities (free text answers)

Identity Verification

Unique Identifier: Provide ability to uniquely identify and track users across the industry.

a way to technologically enforce a "1 per person" limit

Detect automatic connection from a bot

Whether the device is being controlled by automation software

Campaign Binding: With user consent, bind a credential (such as a cookie) to a campaign and or image to ensure it is not compromised at any stage after scanning.

Whether the browser has been modified in some way

For the 'Account Takeover' use case, rank capabilities in order of importance

Note that a lower mean indicates higher importance

Field	Mean
Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device	1.73
Recognize whether the same device is seen again in the context of multiple identities: For example, seeing many different identities' data coming from the same device can be indicative of account take over	2.88
Counters: Ability to keep an approximate count of how often a physical device has done a specific action.	3.27
Geo Attestation: Confirm the geographic location of a specific device	4.50
User Presence: Confirm that a user is present	4.69
Device and Boot attestation: Confirm that the device and OS matches the reported model and version	5.08
Intent: Reason about the degree of coordination among an arbitrary set of users	5.71
Post-boot attestation: Check for up-to-date security patches and known strains of malware	8.20
App/Site attestation: Confirm that the application or website on the device match the application or website reported to the service	8.20
Element Visibility: Confirm that a given visual element actually activated pixels on the device	8.20
Other	1.20
Other	2.50

For the 'Data Scraping' use case, select all relevant capabilities add ones not listed below

Field	Choice Count
Recognize whether the same device is seen again in the context of multiple identities: For example, seeing many different identities' data coming from the same device can be indicative of account take over	11
Counters: Ability to keep an approximate count of how often a physical device has done a specific action	11
Geo Attestation: Confirm the geographic location of a specific device	10
User Presence: Confirm that a user is present	9
Intent: Reason about the degree of coordination among an arbitrary set of users	7
Device and Boot attestation: Confirm that the device and OS matches the reported model and version	7
Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device	7
Element Visibility: Confirm that a given visual element actually activated pixels on the device	3
App/Site attestation: Confirm that the application or website on the device match the application or website reported to the service	3
Post-boot attestation: Check for up-to-date security patches and known strains of malware	3
Other	1
Other	1

Other Capabilities (free text answers)

Whether the device is being controlled by automation software

Whether the browser has been modified in some way

For the 'Data Scraping' use case, rank capabilities in order of importance

Note that a lower mean indicates higher importance

Field	Mean
Counters: Ability to keep an approximate count of how often a physical device has done a specific action	2.44
Recognize whether the same device is seen again in the context of multiple identities: For example, seeing many different identities' data coming from the same device can be indicative of account take over	3.22
Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device	3.33
Intent: Reason about the degree of coordination among an arbitrary set of users	4.00
User Presence: Confirm that a user is present	4.38
Geo Attestation: Confirm the geographic location of a specific device	4.67
Device and Boot attestation: Confirm that the device and OS matches the reported model and version	4.67
Element Visibility: Confirm that a given visual element actually activated pixels on the device	5.50
App/Site attestation: Confirm that the application or website on the device match the application or website reported to the service	7.33
Post-boot attestation: Check for up-to-date security patches and known strains of malware	8.67
Other	1.00
Other	2.00

For the 'Online Spam & Fake Engagement' use case, select all relevant capabilities and add ones not listed below

Field	Choice Count
Geo Attestation: Confirm the geographic location of a specific device	9
Recognize whether the same device is seen again in the context of multiple identities (e.g., Seeing many different identities' data coming from the same device can be indicative of account take over)	8
Counters: Ability to keep an approximate count of how often a physical device has done a specific action.	8
Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device	7
App/Site attestation: Confirm that the application or website on the device match the application or website reported to the service	6
Intent: Reason about the degree of coordination among an arbitrary set of users	6
User Presence: Confirm that a user is present	6
Device and Boot attestation: Confirm that the device and OS matches the reported model and version	6
Element Visibility: Confirm that a given visual element actually activated pixels on the device	4
Post-boot attestation: Check for up-to-date security patches and known strains of malware	3
Other	2
Other	2
Other	1

Other Capabilities (free text answers)

Referer: what site is trying to load static assets?

Whether the device is being controlled by automation software

Domain ownership: does the customer really own a site that is trying to pull in cross-domain assets?

Whether the browser has been modified in some way

For the 'Online Spam & Fake Engagement' use case, rank capabilities in order of importance

Note that a lower mean indicates higher importance

Field	Mean
Counters: Ability to keep an approximate count of how often a physical device has done a specific action.	3.57
Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device	4.00
Recognize whether the same device is seen again in the context of multiple identities (e.g., Seeing many different identities' data coming from the same device can be indicative of account take over)	4.00
App/Site attestation: Confirm that the application or website on the device match the application or website reported to the service	4.40
User Presence: Confirm that a user is present	4.67
Element Visibility: Confirm that a given visual element actually activated pixels on the device	5.00
Device and Boot attestation: Confirm that the device and OS matches the reported model and version	5.50
Intent: Reason about the degree of coordination among an arbitrary set of users	5.80
Geo Attestation: Confirm the geographic location of a specific device	6.43
Post-boot attestation: Check for up-to-date security patches and known strains of malware	8.67
Other	1.00
Other	2.00
Other	9.00

For the 'Invalid Traffic (IVT) in Advertising' use case, select all relevant capabilities and add ones not listed below

Field	Choice Count
Geo Attestation: Confirm the geographic location of a specific device	8
Counters: Ability to keep an approximate count of how often a physical device has done a specific action.	8
Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device	8
Recognize whether the same device is seen again in the context of multiple identities: For example, seeing many different identities' data coming from the same device can be indicative of account take over	7
App/Site attestation: Confirm that the application or website on the device match the application or website reported to the service	7
Element Visibility: Confirm that a given visual element actually activated pixels on the device	6
User Presence: Confirm that a user is present	6
Intent: Reason about the degree of coordination among an arbitrary set of users	5
Device and Boot attestation: Confirm that the device and OS matches the reported model and version	4
Post-boot attestation: Check for up-to-date security patches and known strains of malware	2

For the 'Invalid Traffic (IVT) in Advertising' use case, rank capabilities in order of importance

Note that a lower mean indicates higher importance

Field	Mean
App/Site attestation: Confirm that the application or website on the device match the application or website reported to the service	2.40
Element Visibility: Confirm that a given visual element actually activated pixels on the device	3.40
Counters: Ability to keep an approximate count of how often a physical device has done a specific action.	3.71
Device and Boot attestation: Confirm that the device and OS matches the reported model and version	3.75
Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device	4.29
Geo Attestation: Confirm the geographic location of a specific device	4.33
User Presence: Confirm that a user is present	4.40
Recognize whether the same device is seen again in the context of multiple identities: For example, seeing many different identities’ data coming from the same device can be indicative of account take over	5.40
Post-boot attestation: Check for up-to-date security patches and known strains of malware	7.00
Intent: Reason about the degree of coordination among an arbitrary set of users	7.00

For the 'Unauthorized Access' use case, select all relevant capabilities and add ones not listed below

Field	Choice Count
Recognize whether the same device is seen again in the context of multiple identities (e.g., Seeing many different identities' data coming from the same device can be indicative of account take over)	9
Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device	9
Device and Boot attestation: Confirm that the device and OS matches the reported model and version	8
Geo Attestation: Confirm the geographic location of a specific device	7
User Presence: Confirm that a user is present	6
Counters: Ability to keep an approximate count of how often a physical device has done a specific action.	5
App/Site attestation: Confirm that the application or website on the device match the application or website reported to the service	4
Intent: Reason about the degree of coordination among an arbitrary set of users	4
Post-boot attestation: Check for up-to-date security patches and known strains of malware	3
Element Visibility: Confirm that a given visual element actually activated pixels on the device	1
Other	1

Other Capabilities (free text answers)

Identity Verification

For the 'Unauthorized Access' use case, rank capabilities in order of importance

Note that a lower mean indicates higher importance

Field	Mean
Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device	1.40
Counters: Ability to keep an approximate count of how often a physical device has done a specific action.	3.00
Recognize whether the same device is seen again in the context of multiple identities (e.g., Seeing many different identities' data coming from the same device can be indicative of account take over)	3.00
Intent: Reason about the degree of coordination among an arbitrary set of users	4.33
Device and Boot attestation: Confirm that the device and OS matches the reported model and version	4.60
Geo Attestation: Confirm the geographic location of a specific device	5.20
App/Site attestation: Confirm that the application or website on the device match the application or website reported to the service	5.33
User Presence: Confirm that a user is present	5.40
Post-boot attestation: Check for up-to-date security patches and known strains of malware	7.00
Element Visibility: Confirm that a given visual element actually activated pixels on the device	10.00

For the 'Denial of Service' use case, select capabilities that can address the use case and add ones not listed below

Field	Choice Count
Counters: Ability to keep an approximate count of how often a physical device has done a specific action.	7
Geo Attestation: Confirm the geographic location of a specific device	6
Recognize whether the same device is seen again in the context of multiple identities (e.g., Seeing many different identities' data coming from the same device can be indicative of account take over)	5
Device and Boot attestation: Confirm that the device and OS matches the reported model and version	5
Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device	4
Intent: Reason about the degree of coordination among an arbitrary set of users	3
Post-boot attestation: Check for up-to-date security patches and known strains of malware	3
User Presence: Confirm that a user is present	3
Element Visibility: Confirm that a given visual element actually activated pixels on the device	2
App/Site attestation: Confirm that the application or website on the device match the application or website reported to the service	2
Other	1
Other	1

Other Capabilities (free text answers)

Whether the browser has been modified in some way

Whether the device is being controlled by automation software

---

For the 'Denial of Service' use case, rank capabilities in order of importance

Note that a lower mean indicates higher importance

Field	Mean
Counters: Ability to keep an approximate count of how often a physical device has done a specific action.	2.00
Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device	2.33
Recognize whether the same device is seen again in the context of multiple identities (e.g., Seeing many different identities' data coming from the same device can be indicative of account take over)	2.50
User Presence: Confirm that a user is present	5.00
Device and Boot attestation: Confirm that the device and OS matches the reported model and version	5.33
Geo Attestation: Confirm the geographic location of a specific device	5.50
Intent: Reason about the degree of coordination among an arbitrary set of users	7.00
Post-boot attestation: Check for up-to-date security patches and known strains of malware	7.33
Element Visibility: Confirm that a given visual element actually activated pixels on the device	9.00
App/Site attestation: Confirm that the application or website on the device match the application or website reported to the service	10.00
Other	1.00
Other	2.00

For the 'Theft of Intellectual Property' use case, select all relevant capabilities that can address the use case and add ones not listed below

Field	Choice Count
Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device	4
Recognize whether the same device is seen again in the context of multiple identities (e.g., Seeing many different identities' data coming from the same device can be indicative of account take over)	3
Device and Boot attestation: Confirm that the device and OS matches the reported model and version	3
Geo Attestation: Confirm the geographic location of a specific device	3
Counters: Ability to keep an approximate count of how often a physical device has done a specific action.	3
App/Site attestation: Confirm that the application or website on the device match the application or website reported to the service	2
Intent: Reason about the degree of coordination among an arbitrary set of users	2
Element Visibility: Confirm that a given visual element actually activated pixels on the device	1
Post-boot attestation: Check for up-to-date security patches and known strains of malware	1
User Presence: Confirm that a user is present	1
Other	1
Other	1

Other Capabilities (free text answers)

Whether the device is being controlled by automation software

Whether the browser has been modified in some way

For the 'Theft of Intellectual Property' use case, rank capabilities in order of importance

Note that a lower mean indicates higher importance

Field	Mean
Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device	2.00
Recognize whether the same device is seen again in the context of multiple identities (e.g., Seeing many different identities' data coming from the same device can be indicative of account take over)	2.50
Counters: Ability to keep an approximate count of how often a physical device has done a specific action.	5.00
User Presence: Confirm that a user is present	5.00
Device and Boot attestation: Confirm that the device and OS matches the reported model and version	6.00
Geo Attestation: Confirm the geographic location of a specific device	6.50
Intent: Reason about the degree of coordination among an arbitrary set of users	6.50
App/Site attestation: Confirm that the application or website on the device match the application or website reported to the service	9.00
Post-boot attestation: Check for up-to-date security patches and known strains of malware	10.00
Element Visibility: Confirm that a given visual element actually activated pixels on the device	12.00
Other	1.00
Other	2.00

For 'Other' use cases, select all relevant capabilities that can address the use case and add ones not listed below

Field	Total
Geo Attestation: Confirm the geographic location of a specific device	6
Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device	6
Recognize whether the same device is seen again in the context of multiple identities (e.g., Seeing many different identities' data coming from the same device can be indicative of account take over)	6
Intent: Reason about the degree of coordination among an arbitrary set of users	4
Counters: Ability to keep an approximate count of how often a physical device has done a specific action.	3
Device and Boot attestation: Confirm that the device and OS matches the reported model and version	3
User Presence: Confirm that a user is present	3
App/Site attestation: Confirm that the application or website on the device match the application or website reported to the service	3
Post-boot attestation: Check for up-to-date security patches and known strains of malware	2
Other	3
Other	3

Other Capabilities (free text answers)

Unique Identifier: Provide ability to uniquely identify and track users across the industry.

Campaign Binding: With user consent, bind a credential (such as a cookie) to a campaign and or image to ensure it is not compromised at any stage after scanning.

Unique Identifier: Provide ability to uniquely identify and track users across the industry.

Campaign Binding: With user consent, bind a credential (such as a cookie) to a campaign and or image to ensure it is not compromised at any stage after scanning.

Unique Identifier: Provide ability to uniquely identify and track users across the industry

Campaign Binding: With user consent, bind a credential (such as a cookie) to a campaign and or image to ensure it is not compromised at any stage after scanning

---

If an out-of-band feedback mechanism existed, would you be willing to provide the attestor with feedback (e.g. via RPC) on attestations associated with abuse of your services?

30 Responses