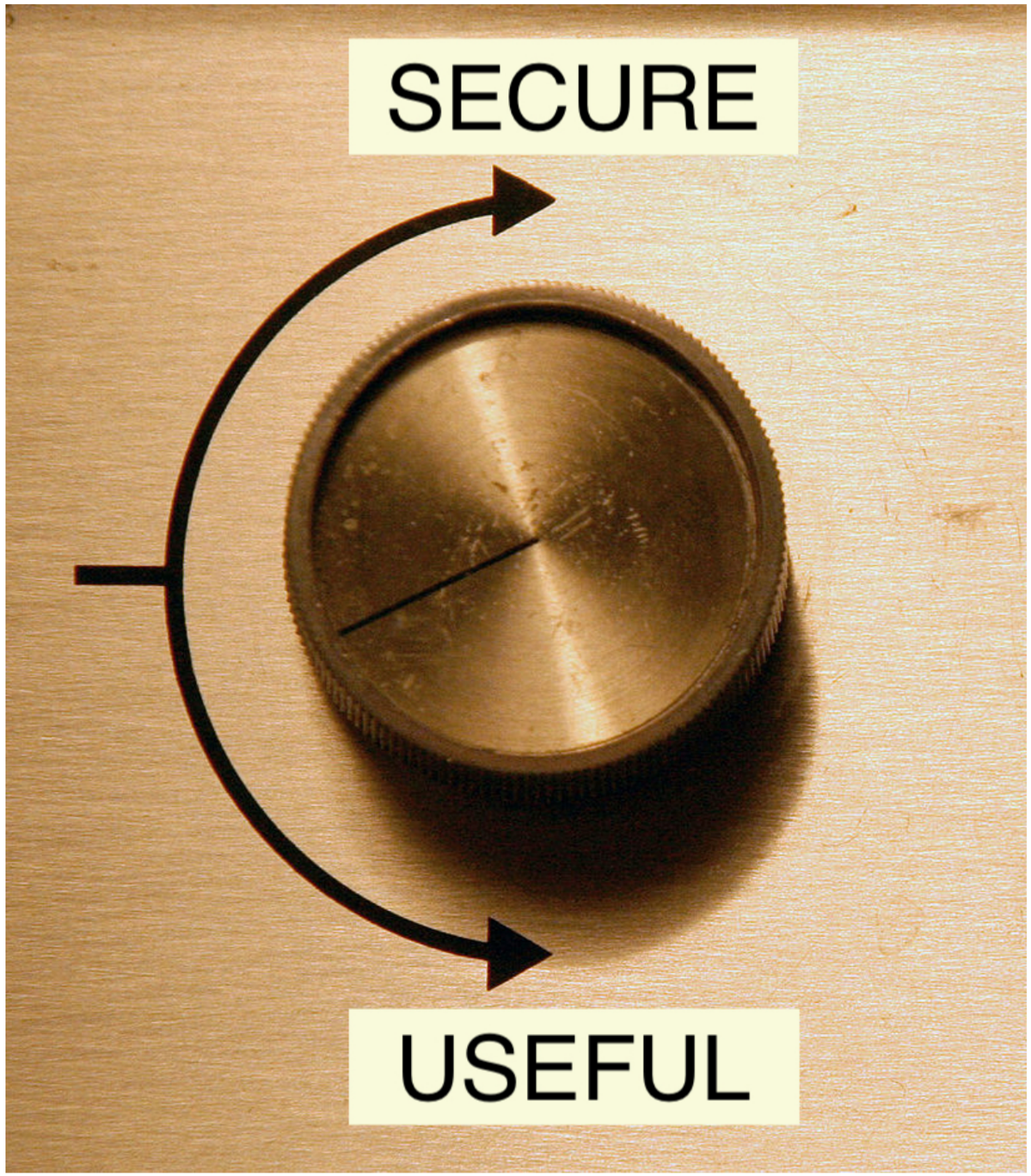
Statistical Analysis of Network Exposure

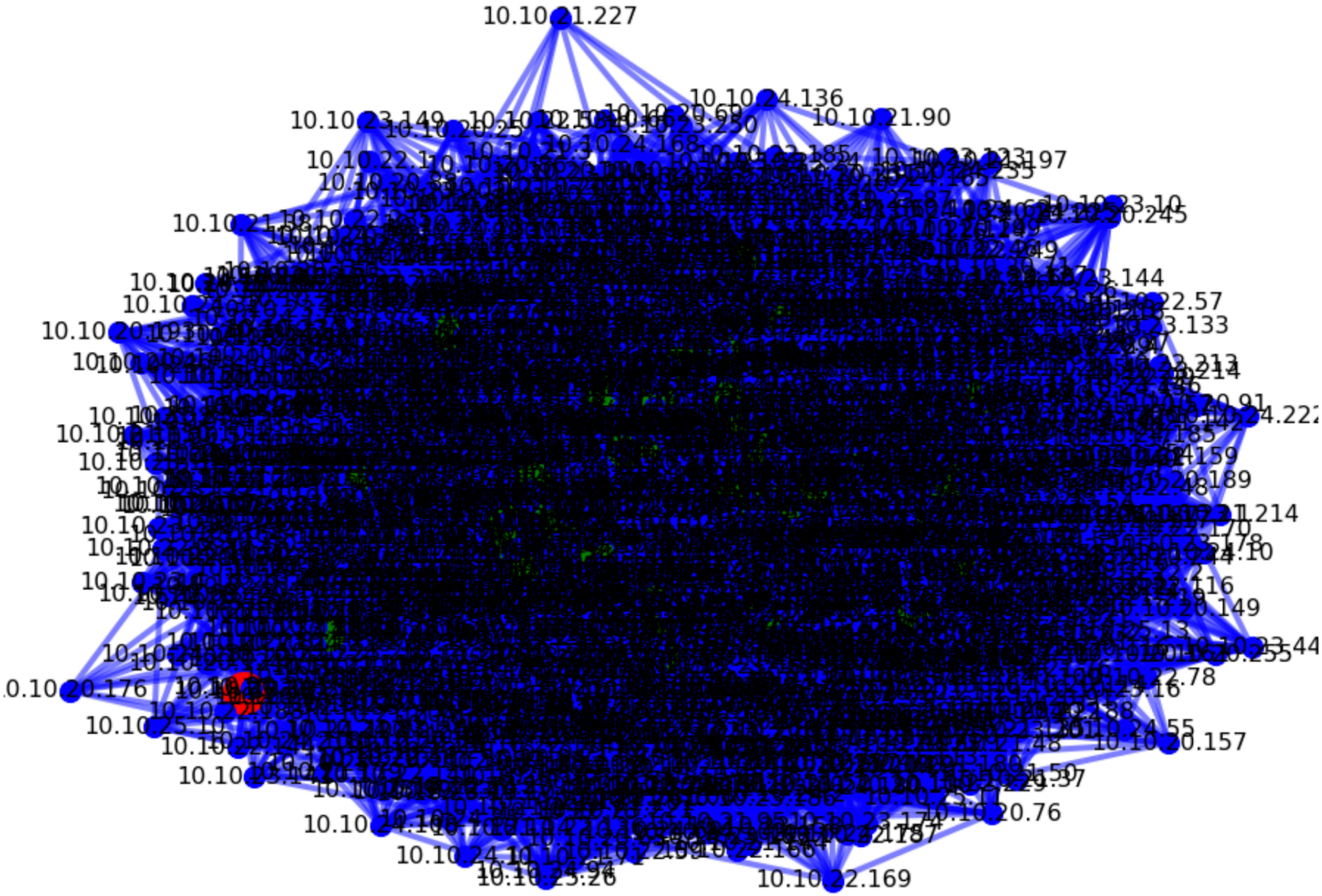
John O'Neil
Chief Data Scientist, Edgewise Networks

Wednesday, 22 May 2019

Most Networks are Vulnerable



Most Networks are Complicated



Solution

- Quantify risk
- Define metrics
- Focus efforts on greatest risk

Outline (Where we're going)

- Analyze several networks, selected from a larger set
  - Based on a few months of data
- Demonstrate overexposure, complexity, other metrics
  - And their relation to security
  - Which is what we want to improve
- Indicate how to improve
  - If we can measure it, we can improve it.

Network Data

- Netflow + app information
  - e.g. incorporate AppIds from NextGen firewalls….
- Distributed NMAP

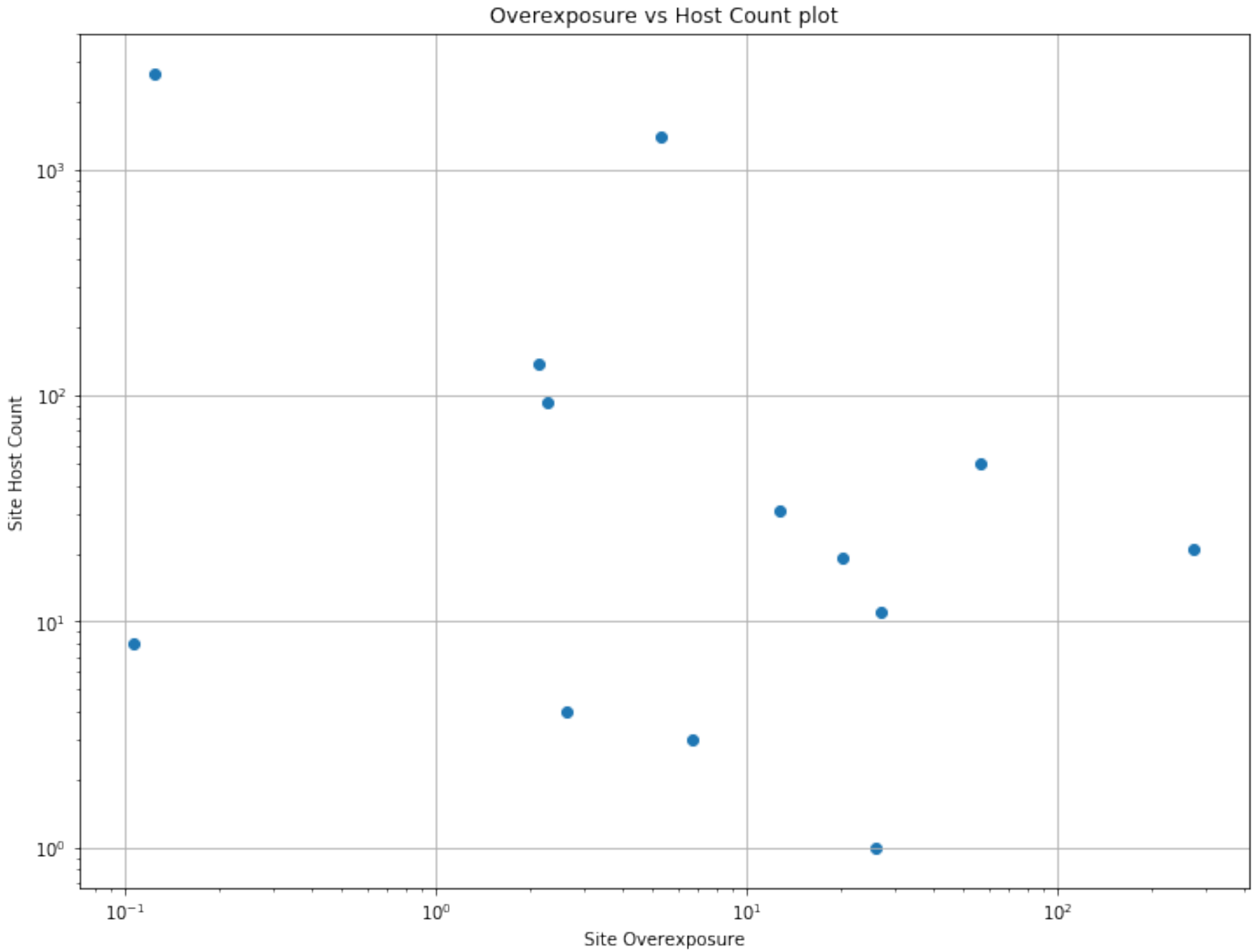
Overexposure

```
IP range,Port range,Protocols,DNS,Specific DNS servers,MAC,OS,
10.10.22.0/24; 10.10.21.0/24,1-11000,TCP,true,from local machine settings,true,true,

Scan Results,
IP,hostname,MAC,OS,Ping,Opened Ports,Closed ports,Filtered ports,
10.10.21.16,,,Windows Server 2008 R2 Datacenter 7601 Service Pack 1 ,0 ms,7,10993,,
Ports,Status,IANA name,
TCP/135,Open,epmap,
TCP/139,Open,netbios-ssn,
TCP/445,Open,microsoft-ds,
TCP/3306,Open,mysql,
TCP/3389,Open,ms-wbt-server,
TCP/5985,Open,wsman,
TCP/5986,Open,wsmans,
```

$$Overexposure = \frac{openPorts - neededPorts}{neededPorts}$$

Overexposure Site Data



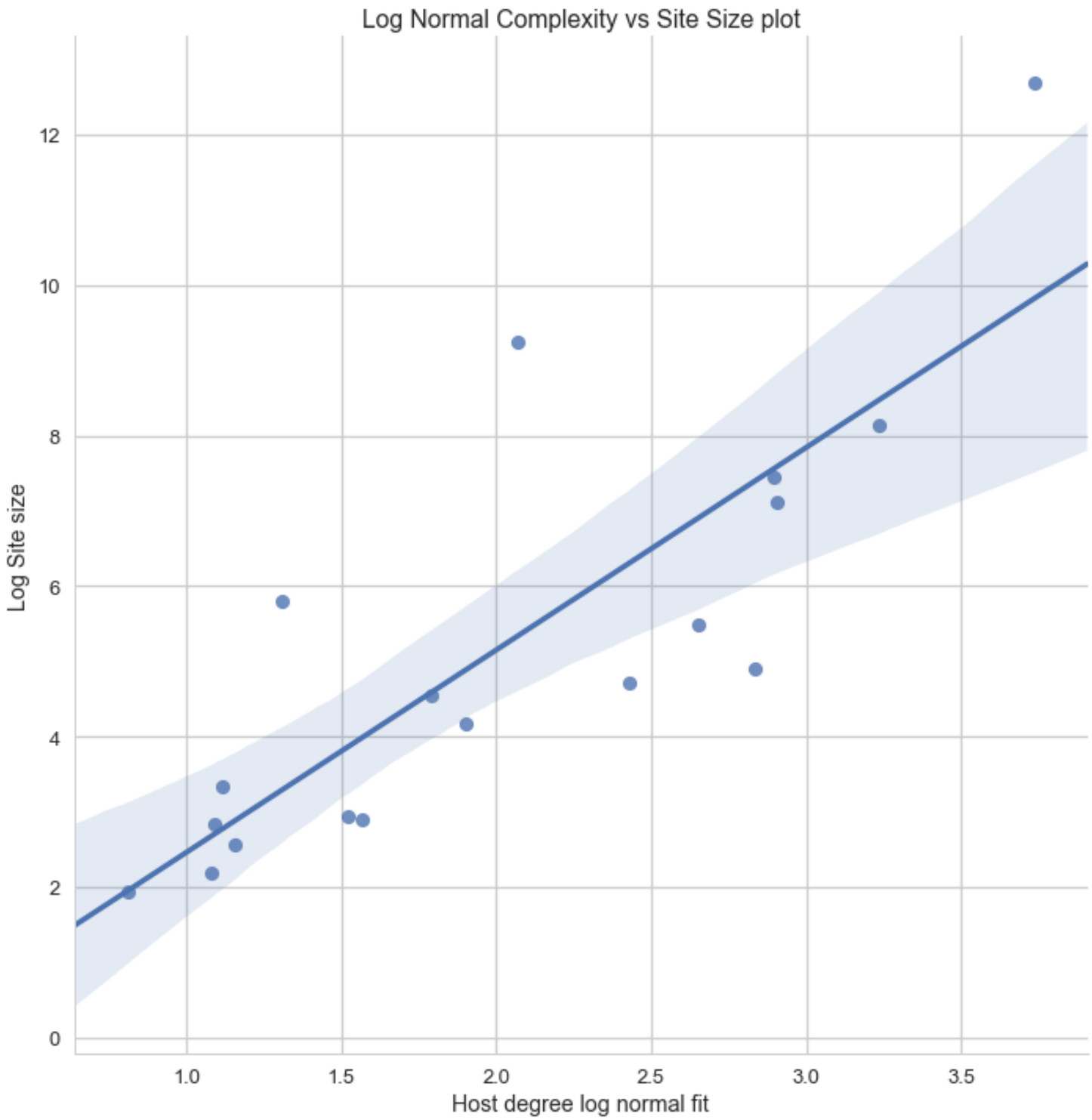
Complexity, v. 1

Fit node degree (# edges into/out of a host) as a **log-normal** distribution

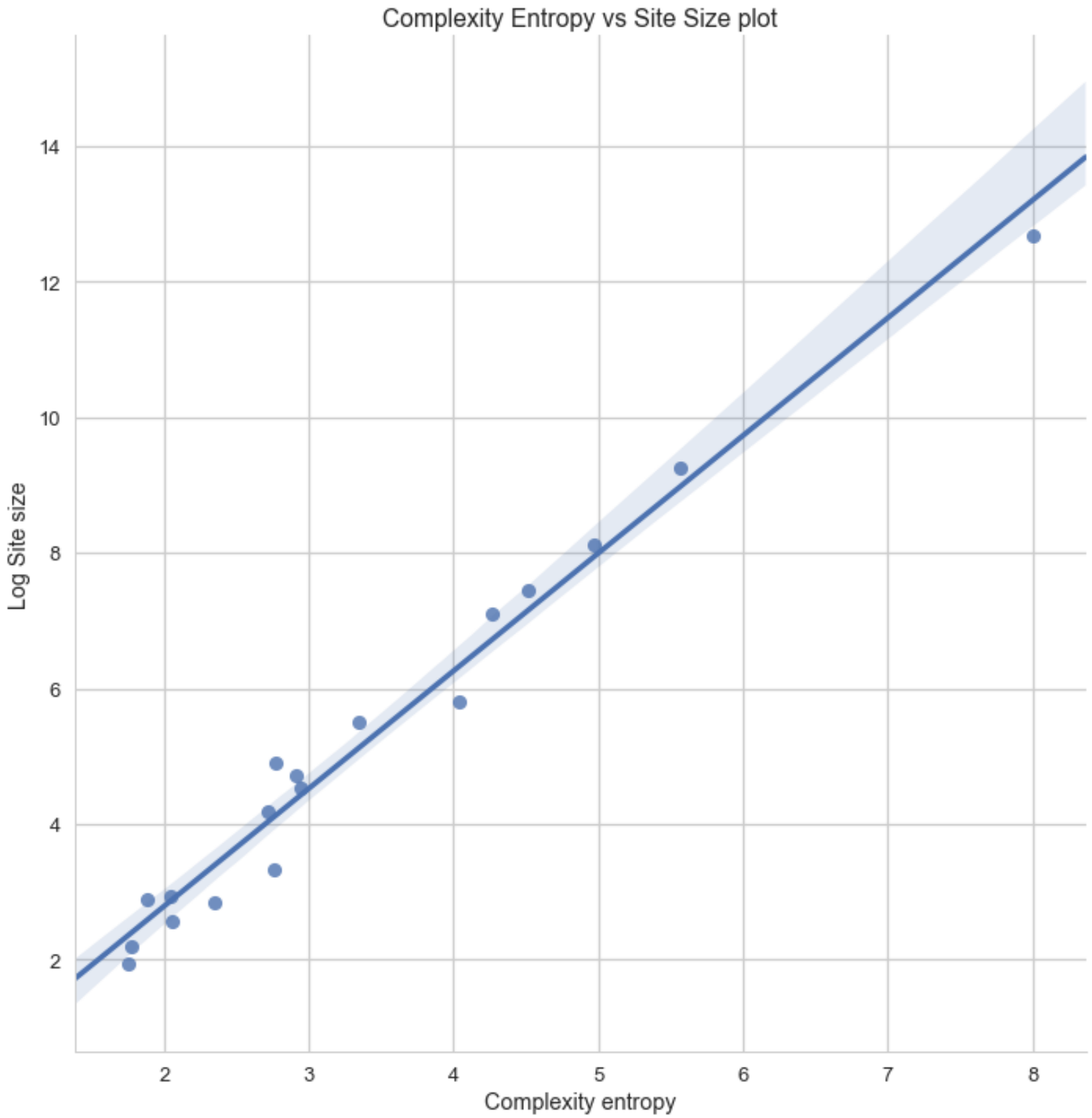
$$\hat{\mu} = \frac{1}{n} \sum_{k} \ln x_k$$

$$\hat{\sigma}^2 = \frac{1}{n} \left(\sum_{k} \ln x_k - \hat{\mu} \right)$$

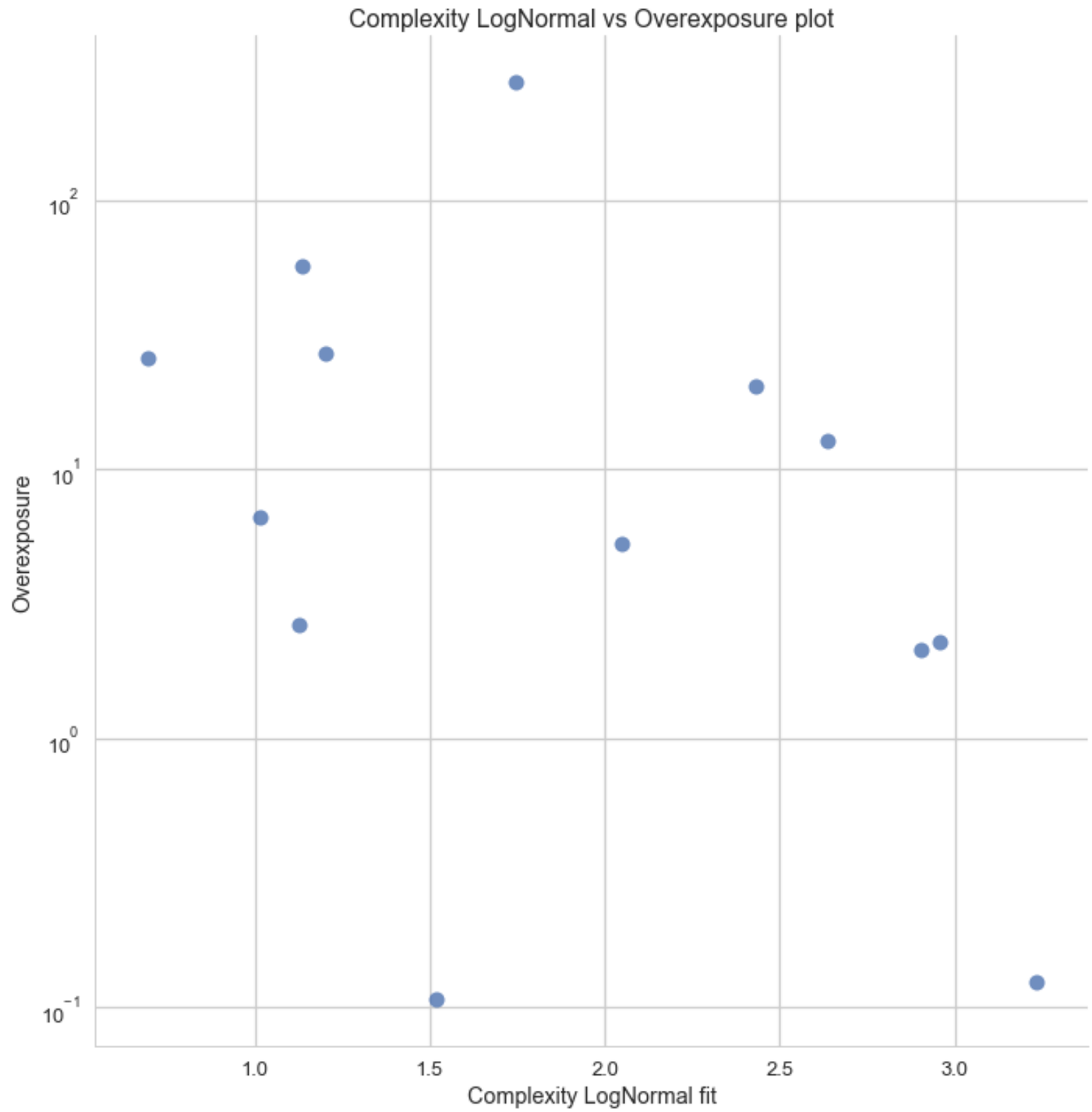
Complexity Site Data



Entropy, too


Complexity Entropy vs Site Size plot
Log Site size
14
12
10
8
6
4
2
2
3
4
5
6
7
8
Complexity entropy

Complexity vs Overexposure



Networks Change

- Perfect policies today but not tomorrow
- Adaptive policies - agile network security
- Continuous monitoring

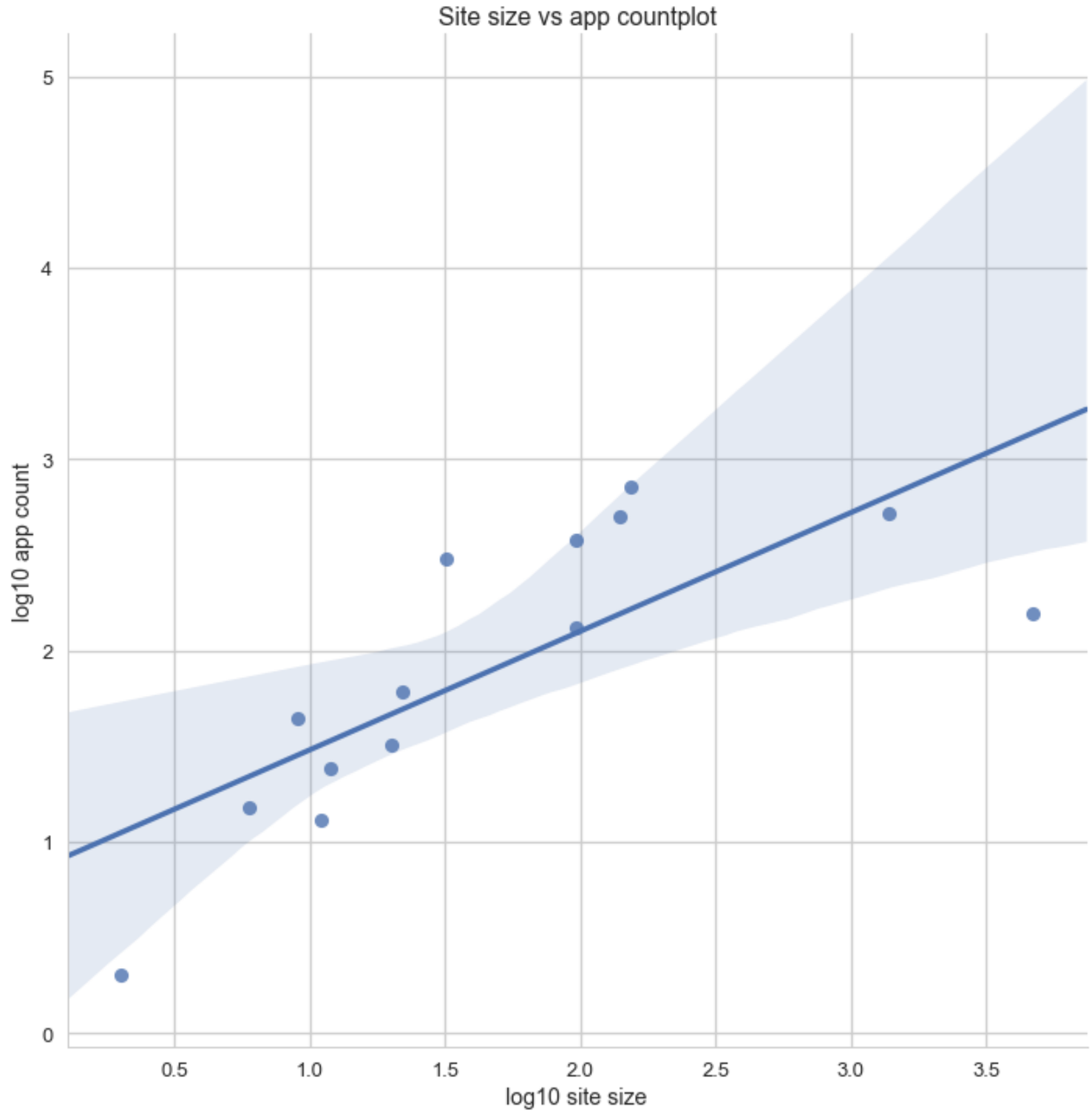
Host Statistics for Sites

siteId	host count	mean apps/host	stdev apps/host	min apps/host	median apps/host	max apps/host
0121	143	31.5245	14.1291	4	28	97
3ebb	18	4.72222	3.6911	1	3	13
4999	7	13.1429	3.57904	8	14	19
6654	11	4	2.04939	2	3	9
99f9	88	18.8636	13.2944	1	18	73
9b04	21	5.14286	1.95667	2	5	11
bc31	31	19.3548	43.3048	4	8	190
bd92	1002	10.6527	5.03307	0	11	64
c742	132	20.4924	9.04399	9	19	48
cbe7	52	4.55769	2.55461	1	4	12
f368	1034	5.89458	4.15893	1	5	18

Host Statistics for Sites

siteId	host count	mean apps/host	stdev apps/host	min apps/host	median apps/host	max apps/host
0121	143	31.5245	14.1291	4	28	97
3ebb	18	4.72222	3.6911	1	3	13
4999	7	13.1429	3.57904	8	14	19
6654	11	4	2.04939	2	3	9
99f9	88	18.8636	13.2944	1	18	73
9b04	21	5.14286	1.95667	2	5	11
bc31	31	19.3548	43.3048	4	8	190
bd92	1002	10.6527	5.03307	0	11	64
c742	132	20.4924	9.04399	9	19	48
cbe7	52	4.55769	2.55461	1	4	12
f368	1034	5.89458	4.15893	1	5	18

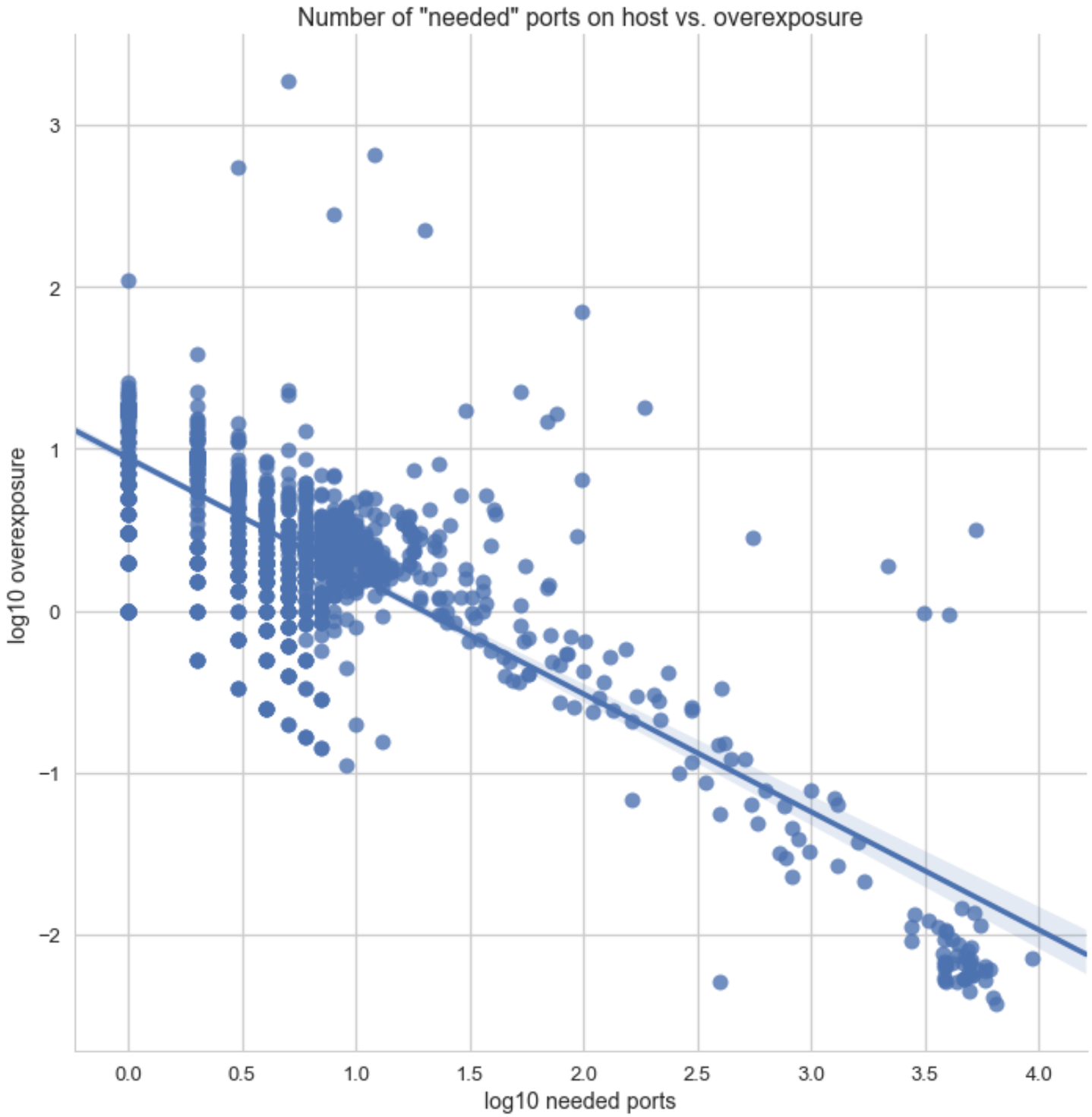
Site Size & App Growth



Host and Application Overexposure

- Combine host/port/app information
- Get app exposure across network
- Numeric value → prioritization

Host Overexposure



App Overexposure Across Site

siteId	appName	overexposure
0121	svchost.exe	26365
0121	System	26363
0121	vncserver.exe	581
0121	ndclickwintray.exe	165
28be	python3	13
28be	ir_agent	13
28be	consul	13
3ebb	consul	170
4999	System	220
4999	swi_fc.exe	200
4999	sqlservr.exe	167
4999	routernt.exe	167
4999	ir_agent.exe	63

siteId	appName	overexposure
6654	svchost.exe	93
7f1c	httpd	3
99f9	nseserv	8
9b04	System	75
bc31	java	42
bc31	python2.7	24
bd92	System	1536
c742	prunsrv.exe	37
cbe7	zabbix_agentd	9780
f368	python2.7	2547
f97a	scribed	8

App Overexposure on Hosts 1

siteId	agentId	appName	overexposure
0121	b105a1f4-2db8-476b-bb2a-690e341aabe3	veeamagent.exe	13545
0121	b105a1f4-2db8-476b-bb2a-690e341aabe3	veeam.guest.interaction.proxy.exe	13545
0121	b105a1f4-2db8-476b-bb2a-690e341aabe3	swi_fc.exe	13545
0121	b105a1f4-2db8-476b-bb2a-690e341aabe3	svchost.exe	13545
0121	b105a1f4-2db8-476b-bb2a-690e341aabe3	routernt.exe	13545
28be	977e438b-7550-4be3-b81d-461bd1c9d7e1	vmware-csd.exe	55
28be	977e438b-7550-4be3-b81d-461bd1c9d7e1	swi_fc.exe	55
28be	977e438b-7550-4be3-b81d-461bd1c9d7e1	routernt.exe	55
28be	2bcf57a0-ecfd-41ae-95c4-21bc723a6c3b	python3	13
28be	2bcf57a0-ecfd-41ae-95c4-21bc723a6c3b	ir_agent	13
3ebb	93a409bc-349a-47ce-918d-7340cd12e91d	sshd	9403
3ebb	93a409bc-349a-47ce-918d-7340cd12e91d	python2.7	9403
3ebb	93a409bc-349a-47ce-918d-7340cd12e91d	java	9403
3ebb	79940591-988e-4869-bebc-aa5b5b207e65	sshd	88
3ebb	79940591-988e-4869-bebc-aa5b5b207e65	python2.7	88
4999	a189d755-5ec3-4ef1-aa18-f03ef684de41	swi_fc.exe	151
4999	a189d755-5ec3-4ef1-aa18-f03ef684de41	sqlservr.exe	151
4999	a189d755-5ec3-4ef1-aa18-f03ef684de41	routernt.exe	151
4999	a189d755-5ec3-4ef1-aa18-f03ef684de41	java.exe	151
4999	a189d755-5ec3-4ef1-aa18-f03ef684de41	httpd.exe	151

App Overexposure on Hosts 2

siteId	agentId	appName	overexposure
6654	fe390825-0abf-4ca2-bffa-37b944d2d926	svchost.exe	35
6654	fe390825-0abf-4ca2-bffa-37b944d2d926	lsass.exe	35
6654	fe390825-0abf-4ca2-bffa-37b944d2d926	dns.exe	35
6654	fe390825-0abf-4ca2-bffa-37b944d2d926	System	35
6654	6fa0c6e1-9dcd-45fe-ac6e-94fd5cd8c2ab	svchost.exe	31
7f1c	dd6761d5-ca95-4874-9bde-c8f9c0c9b27d	svchost.exe	26
7f1c	dd6761d5-ca95-4874-9bde-c8f9c0c9b27d	lsass.exe	26
7f1c	dd6761d5-ca95-4874-9bde-c8f9c0c9b27d	dns.exe	26
7f1c	dd6761d5-ca95-4874-9bde-c8f9c0c9b27d	dfsrs.exe	26
7f1c	dd6761d5-ca95-4874-9bde-c8f9c0c9b27d	System	26
99f9	719ee207-710c-466d-8e12-b93275f93e78	svchost.exe	520
99f9	719ee207-710c-466d-8e12-b93275f93e78	supportassistagent.exe	520
99f9	719ee207-710c-466d-8e12-b93275f93e78	pcdrwi.exe	520
99f9	719ee207-710c-466d-8e12-b93275f93e78	mdnsresponder.exe	520
99f9	719ee207-710c-466d-8e12-b93275f93e78	macmnsvc.exe	520
9b04	07933dce-fba2-4621-b883-be4dd7286ee3	svchost.exe	32
9b04	07933dce-fba2-4621-b883-be4dd7286ee3	lsass.exe	32
9b04	07933dce-fba2-4621-b883-be4dd7286ee3	dns.exe	32
9b04	07933dce-fba2-4621-b883-be4dd7286ee3	dfsrs.exe	32
9b04	07933dce-fba2-4621-b883-be4dd7286ee3	System	32

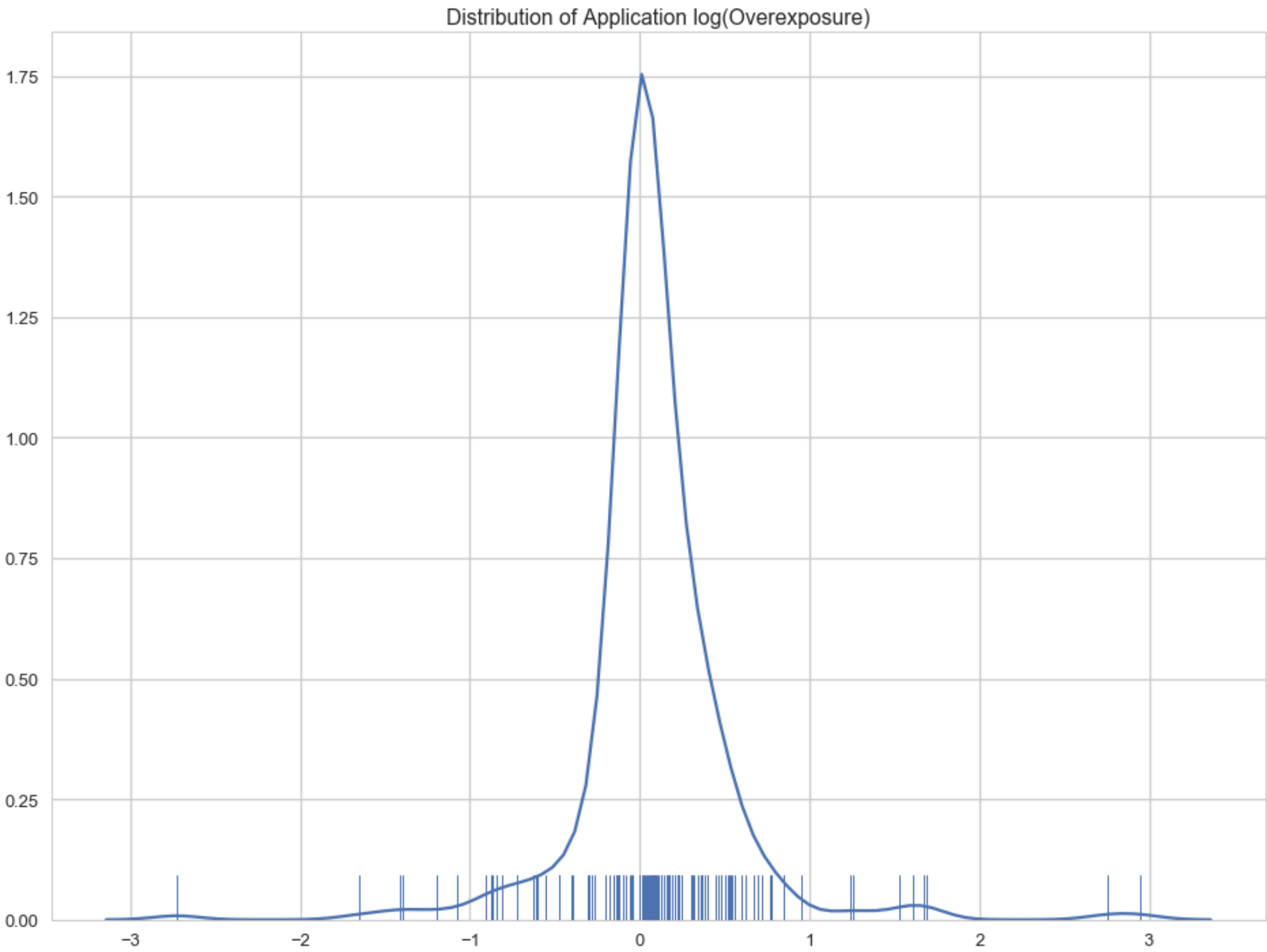
App Overexposure on Hosts 3

siteId	agentId	appName	overexposure
bc31	49d298bb-0cad-4503-9b8b-6015e8d454e4	zabbix_agentd	1657
bc31	49d298bb-0cad-4503-9b8b-6015e8d454e4	sshd	1657
bc31	49d298bb-0cad-4503-9b8b-6015e8d454e4	smtpd	1657
bc31	b7e5d8d8-d060-4f14-aaa5-9ff8157a2c45	zabbix_agentd	102
bc31	b7e5d8d8-d060-4f14-aaa5-9ff8157a2c45	wordSegmentationServer_c6.6155	102
bd92	58396668-a651-4537-b044-612590ca9a23	tentacle.exe	133
bd92	58396668-a651-4537-b044-612590ca9a23	svchost.exe	133
bd92	58396668-a651-4537-b044-612590ca9a23	pccnt.exe	133
bd92	58396668-a651-4537-b044-612590ca9a23	dotnet.exe	133
bd92	58396668-a651-4537-b044-612590ca9a23	System	133
c742	da1f36bf-a71e-4a6a-85f8-c48b3befa927	w3wp.exe	16557
c742	da1f36bf-a71e-4a6a-85f8-c48b3befa927	svchost.exe	16557
c742	da1f36bf-a71e-4a6a-85f8-c48b3befa927	storageonlineopns.exe	16557
c742	da1f36bf-a71e-4a6a-85f8-c48b3befa927	services.exe	16557
c742	da1f36bf-a71e-4a6a-85f8-c48b3befa927	indexer-service.exe	16557
cbe7	76c3db70-f228-4b38-a05d-5220c8981494	zabbix_agentd	6980
cbe7	76c3db70-f228-4b38-a05d-5220c8981494	java (deleted)	6980
cbe7	76c3db70-f228-4b38-a05d-5220c8981494	java	6980
cbe7	76c3db70-f228-4b38-a05d-5220c8981494	elasticsearch	6980
cbe7	204a58eb-c2d0-48c2-878d-e63b211ead89	zabbix_agentd	1250

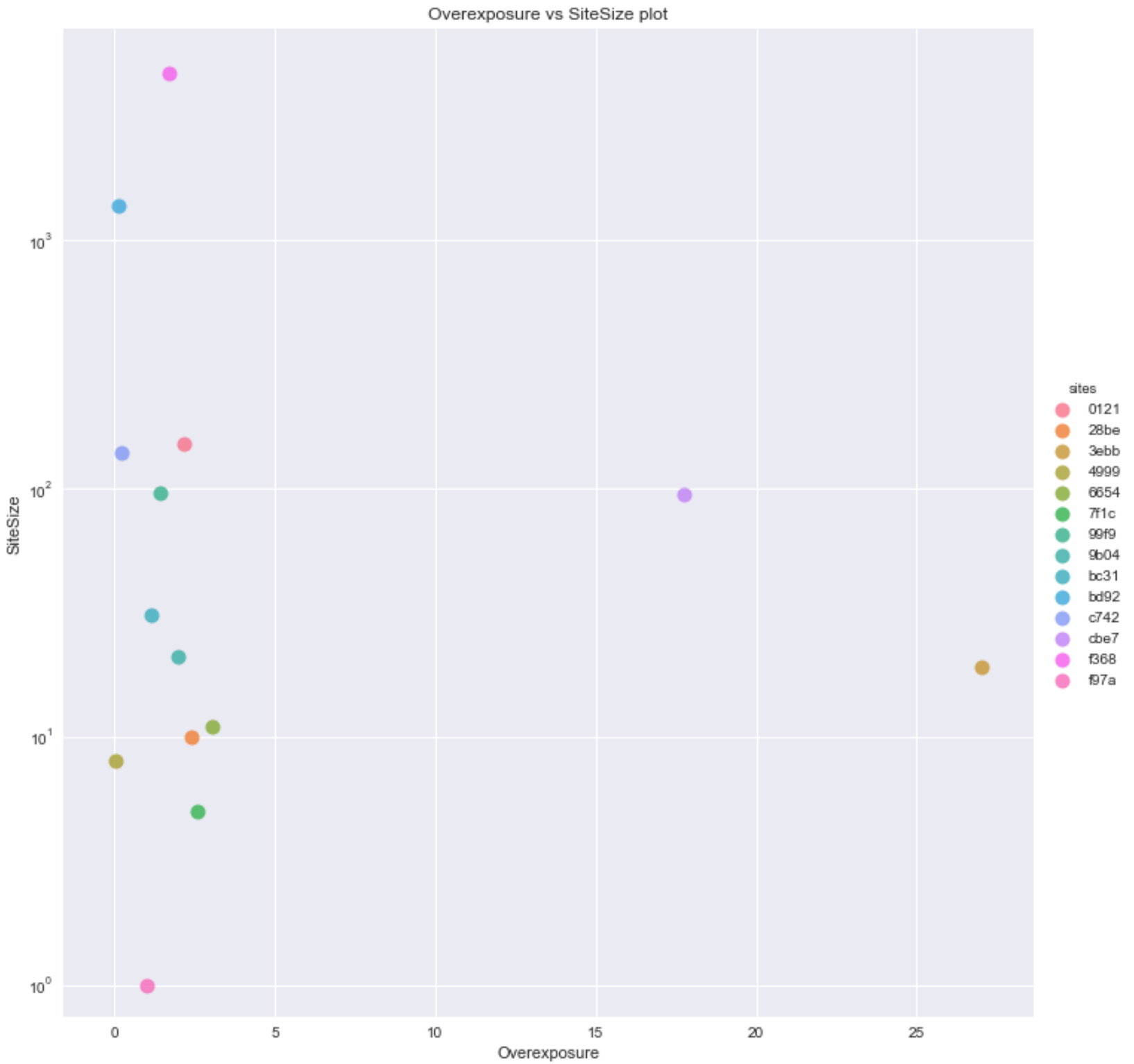
App Overexposure on Hosts 4

siteId	agentId	appName	overexposure
f368	a4f3482d-a3a4-435f-a563-219dc3036340	sshd	2254
f368	a4f3482d-a3a4-435f-a563-219dc3036340	postgres	2254
f368	a4f3482d-a3a4-435f-a563-219dc3036340	java	2254
f368	a4f3482d-a3a4-435f-a563-219dc3036340	httpd	2254
f368	a4f3482d-a3a4-435f-a563-219dc3036340	consul	2254
f97a	b7ab2501-6d02-434d-b19a-6afeb64d9981	scribed	8

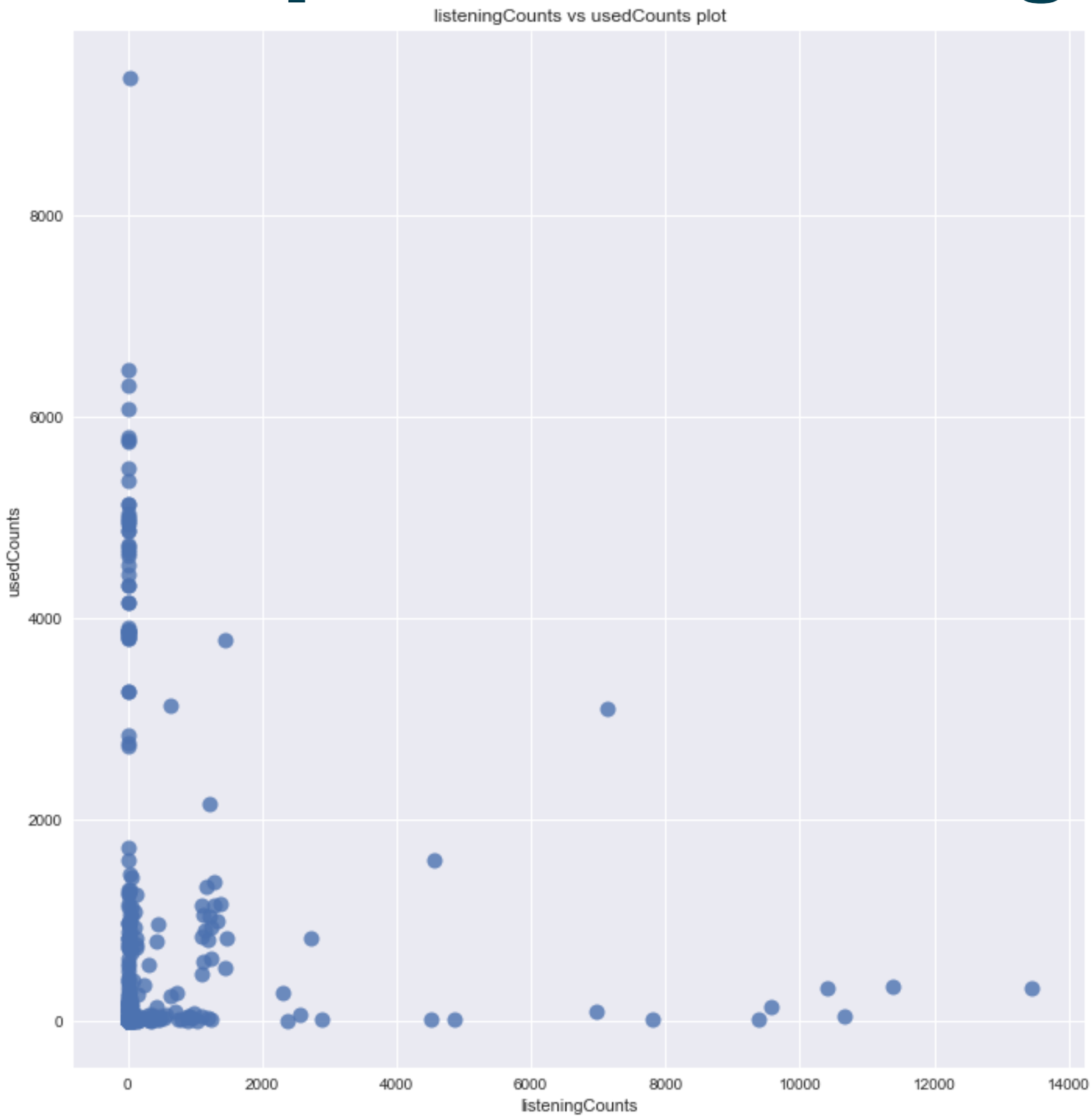
Application Overexposure Distribution



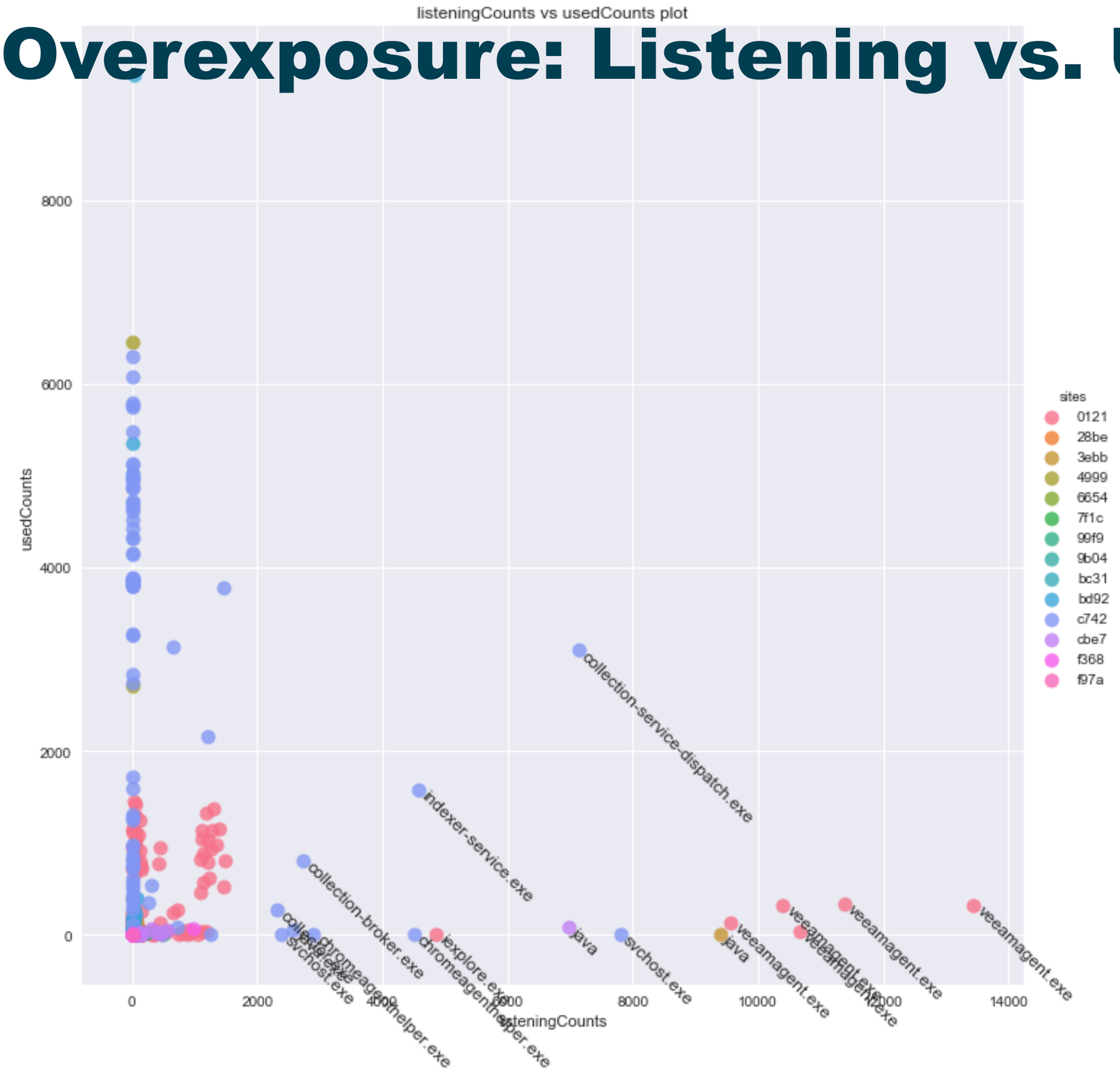
Application Overexposure By Site



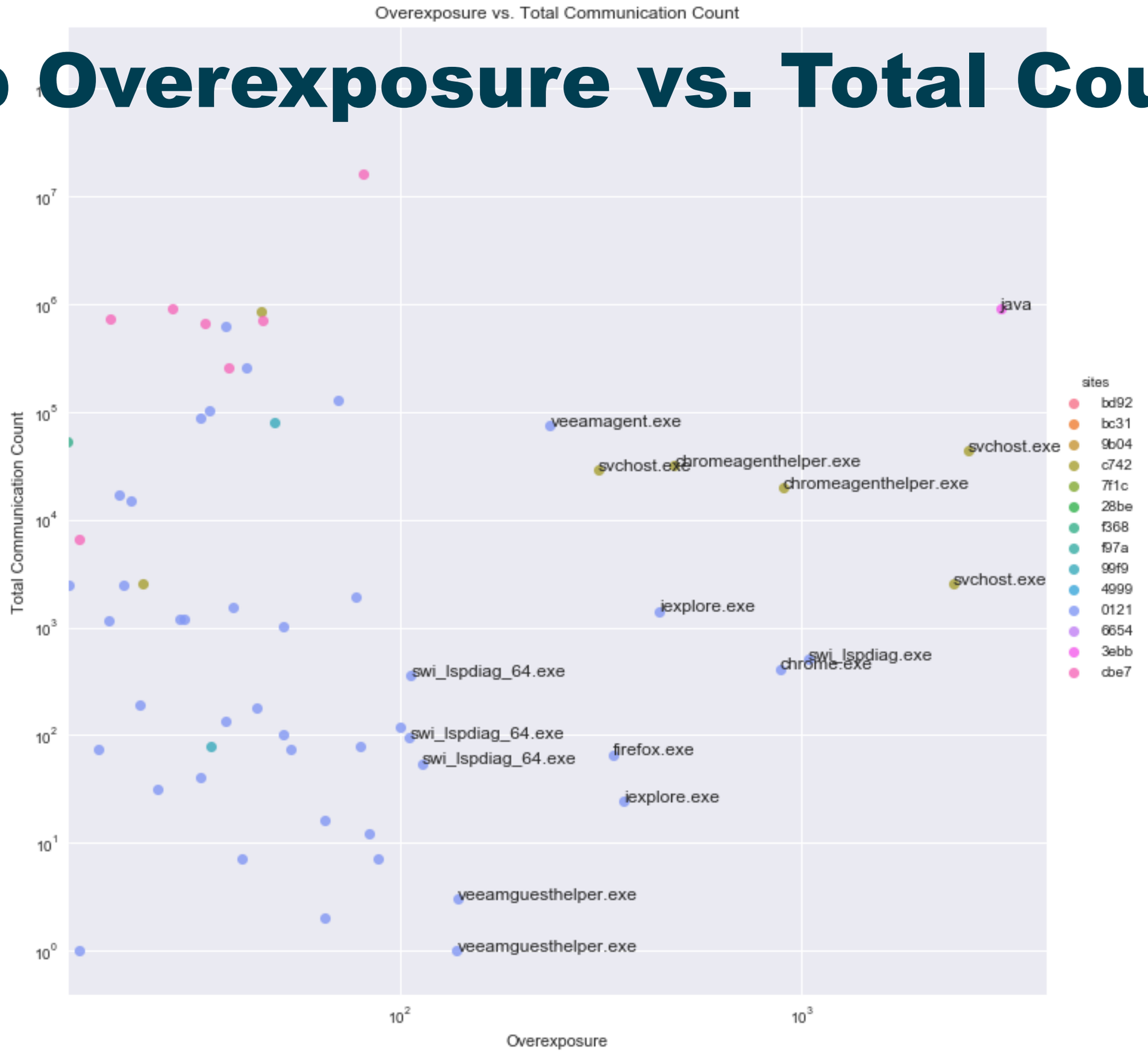
App Overexposure: Listening vs. Used



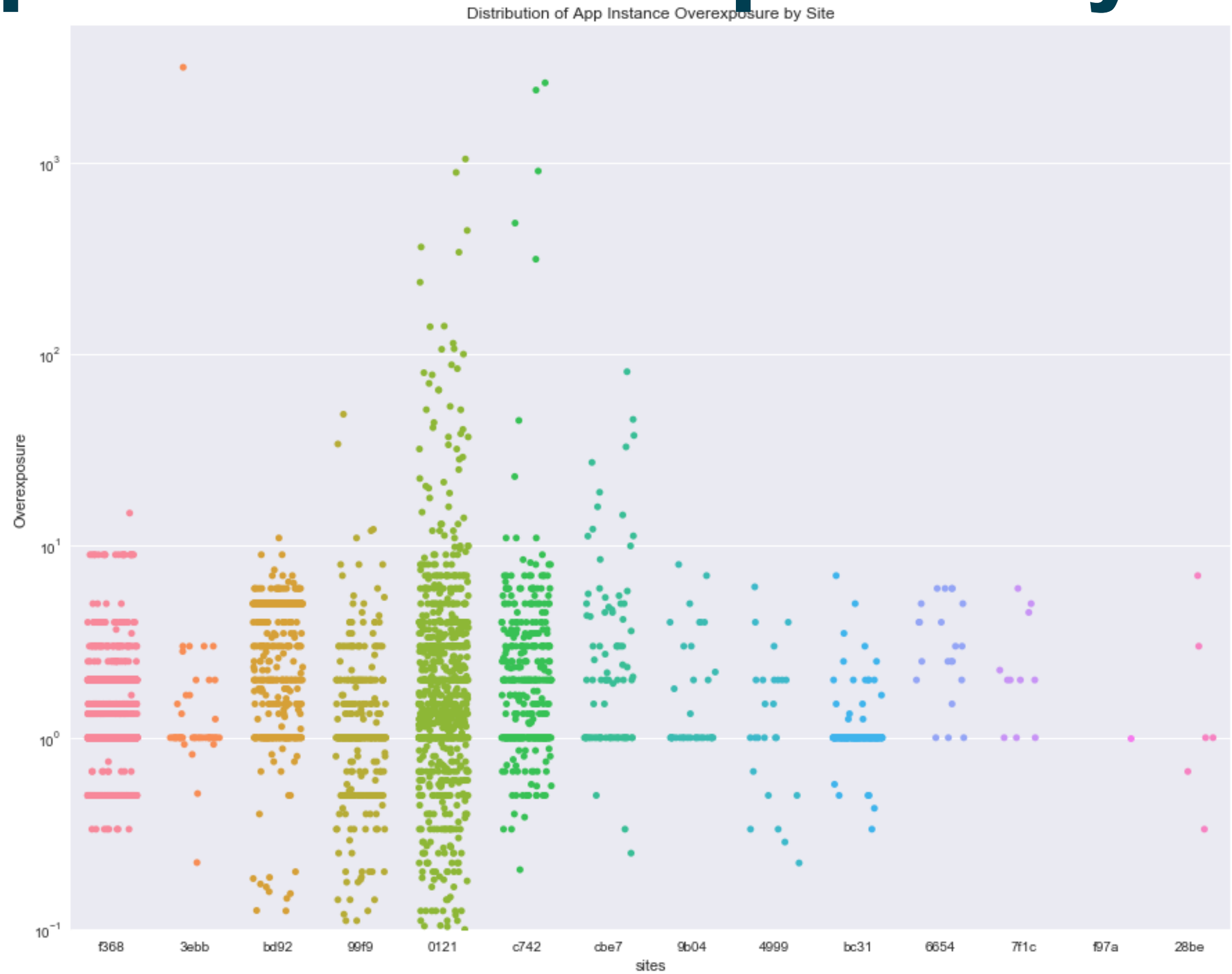
App Overexposure: Listening vs. Used



App Overexposure vs. Total Count



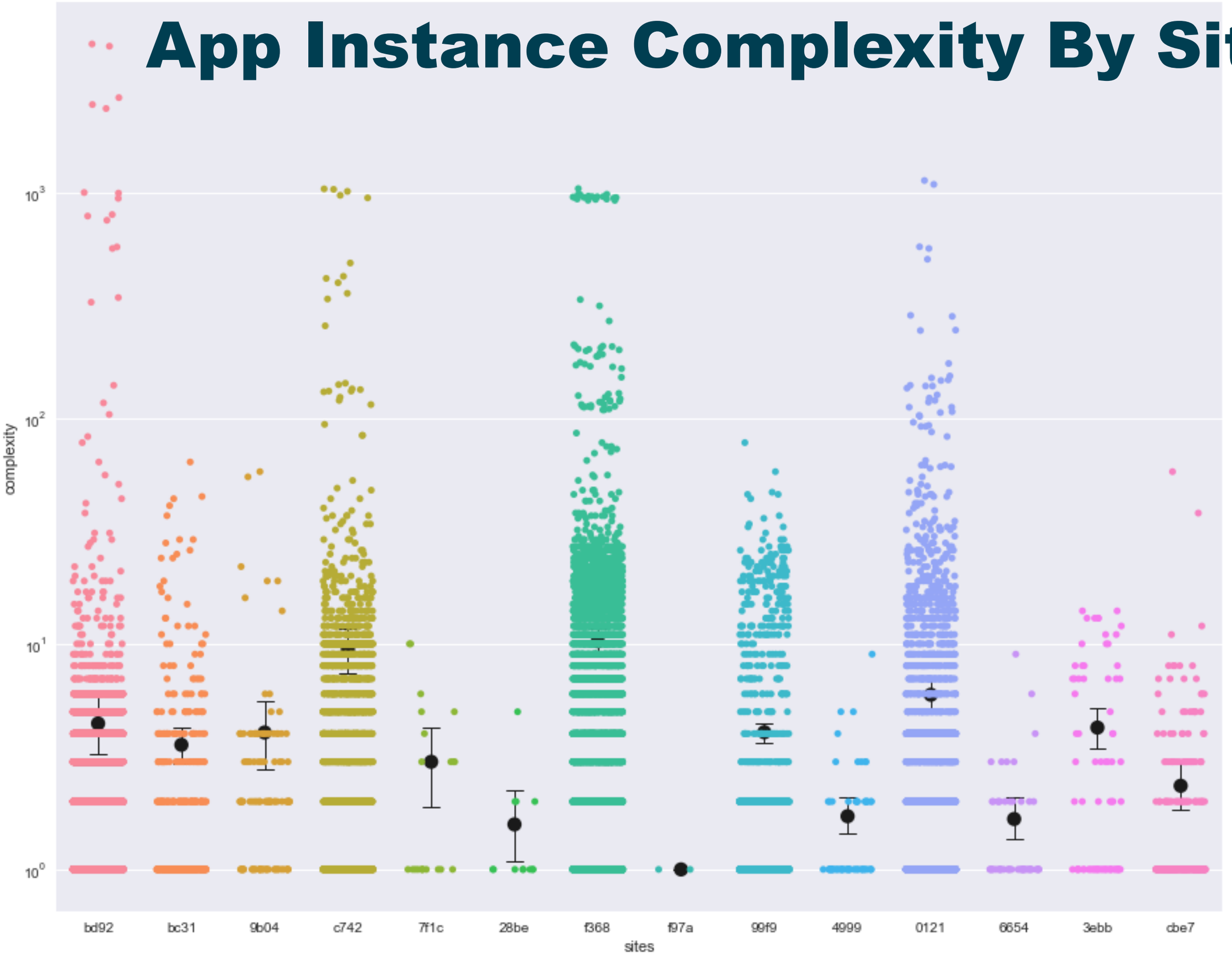
App Instance Overexposure By Site

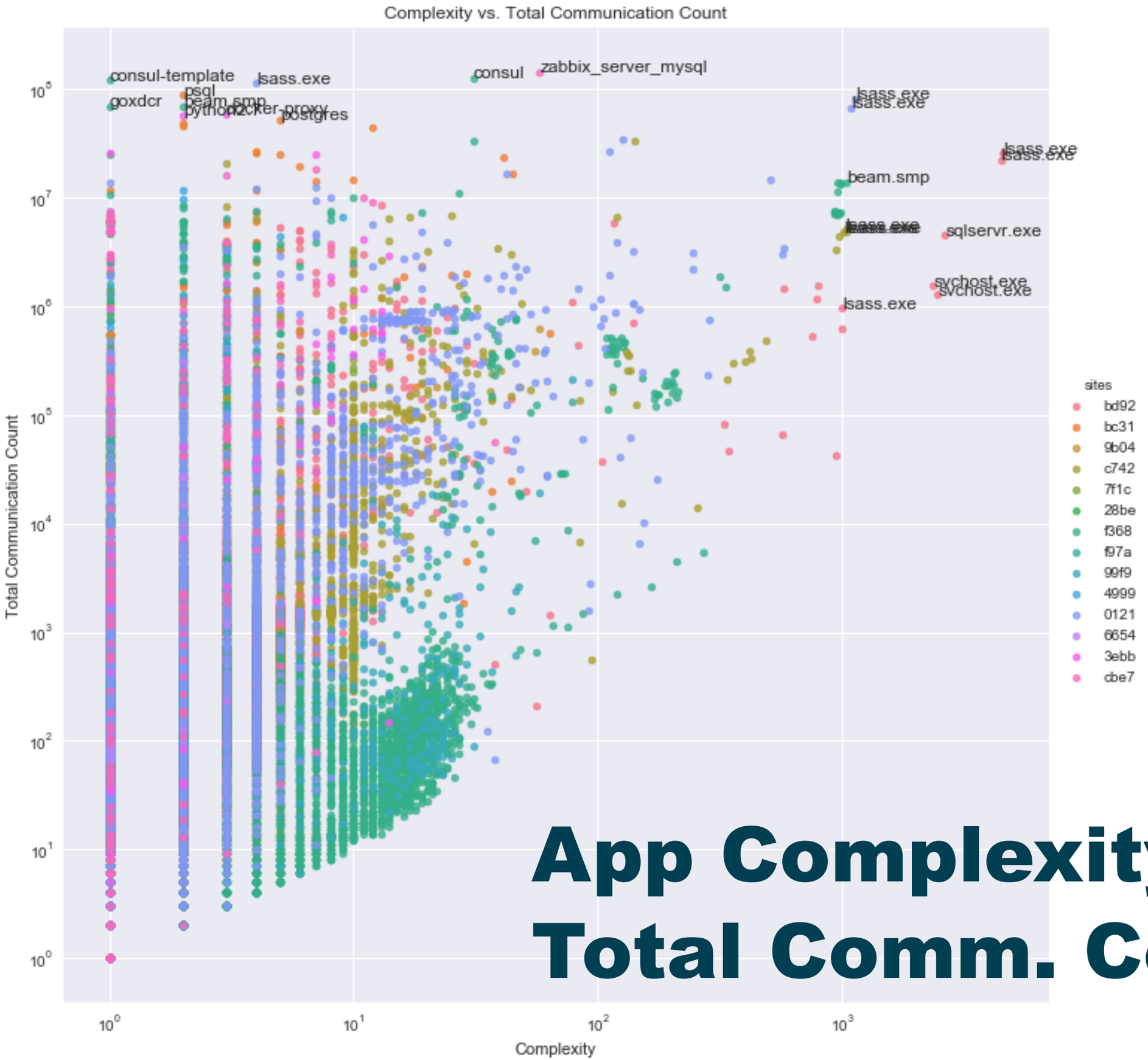


App Instance Overexposure, Lognormal Fit

site	exp(m)	5%	95%	mean	stdev
0121	1.562	0.085	28.543	0.446	1.453
28be	1.293	0.145	11.496	0.257	1.093
3ebb	1.375	0.115	16.479	0.318	1.242
4999	0.630	0.010	38.677	-0.463	2.059
6654	2.878	0.865	9.570	1.057	0.601
7f1c	2.163	0.602	7.776	0.772	0.640
99f9	1.012	0.152	6.743	0.012	0.948
9b04	1.578	0.420	5.926	0.456	0.662
bc31	1.054	0.560	1.983	0.053	0.316
bd92	2.445	0.263	22.724	0.894	1.115
c742	**0.718**	**0.003**	**161.321**	**-0.332**	**2.708**
cbe7	2.450	0.241	24.853	0.896	1.159
f368	1.241	0.478	3.221	0.216	0.477

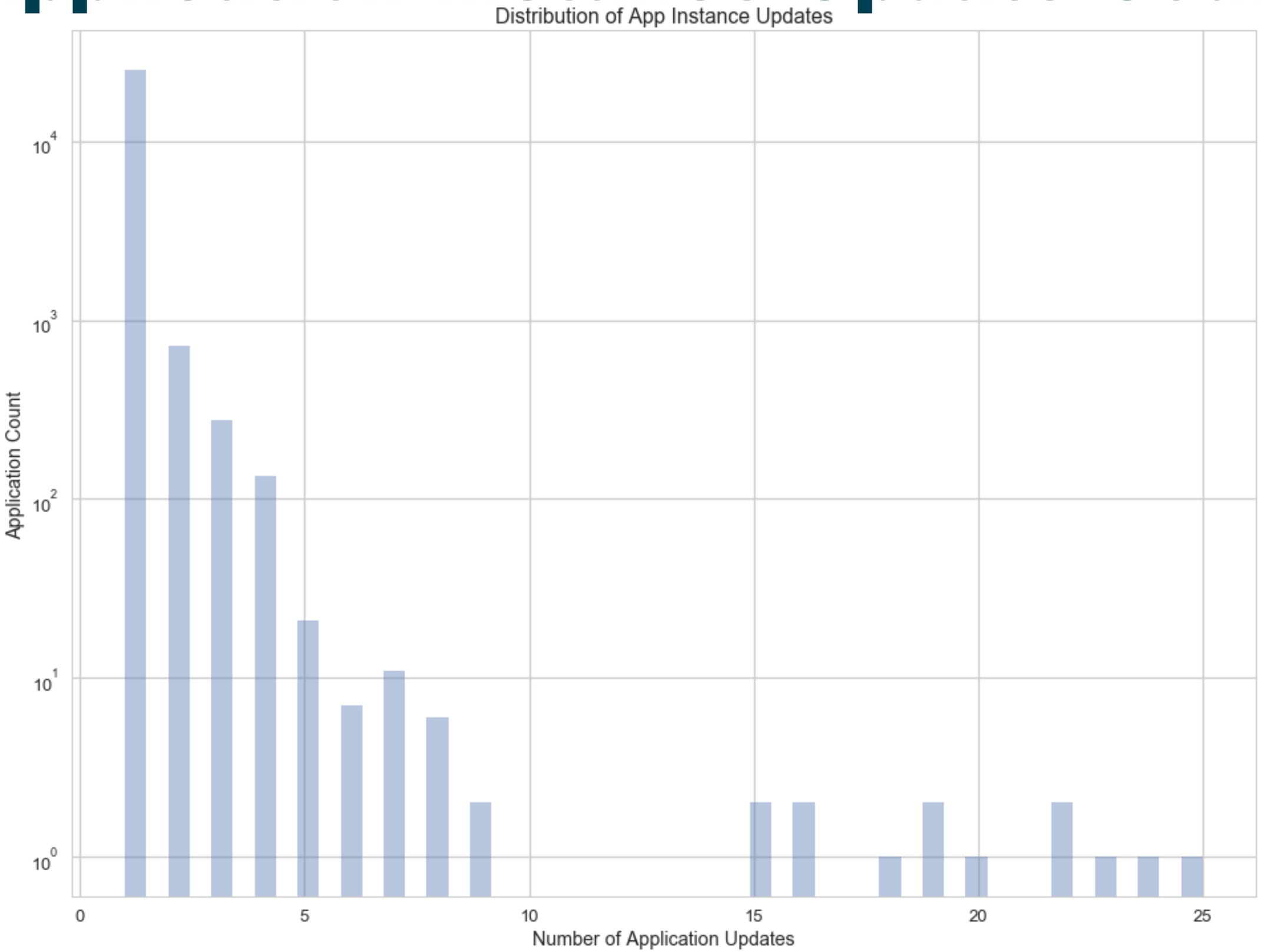
App Instance Complexity By Site



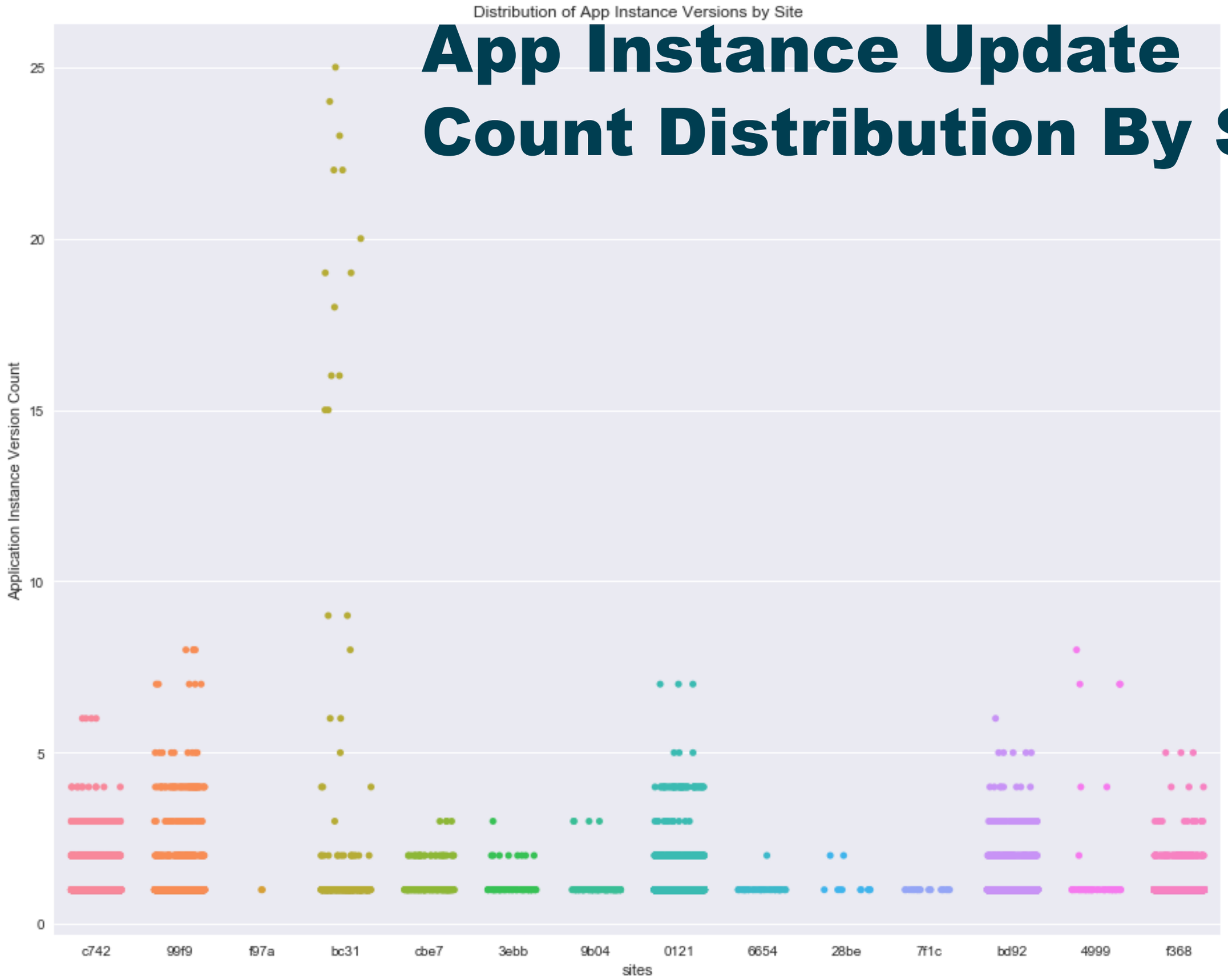


App Complexity vs. Total Comm. Count

Application Instance Update Counts



App Instance Update Count Distribution By Site



Most Updated Applications Over All Sites

site	agent_id	app_name	updates
bc31	b7e5d8d8-d060-4f14-aaa5-9ff8157a2c45	ares	25
bc31	b7e5d8d8-d060-4f14-aaa5-9ff8157a2c45	ares_tii	24
bc31	a95fadb3-7f33-4158-9533-0c593afb21cc	ares	23
bc31	b7e5d8d8-d060-4f14-aaa5-9ff8157a2c45	panda	22
bc31	a95fadb3-7f33-4158-9533-0c593afb21cc	panda	22
bc31	b7e5d8d8-d060-4f14-aaa5-9ff8157a2c45	ares_tiiuk	20
bc31	b7e5d8d8-d060-4f14-aaa5-9ff8157a2c45	ares_translated	19
bc31	b7e5d8d8-d060-4f14-aaa5-9ff8157a2c45	ares_ithenticate	19
bc31	b7e5d8d8-d060-4f14-aaa5-9ff8157a2c45	ares_writecheck	18
bc31	a95fadb3-7f33-4158-9533-0c593afb21cc	palantir	16
bc31	a95fadb3-7f33-4158-9533-0c593afb21cc	nos	16
bc31	b7e5d8d8-d060-4f14-aaa5-9ff8157a2c45	nos	15
bc31	b7e5d8d8-d060-4f14-aaa5-9ff8157a2c45	palantir	15
bc31	b7e5d8d8-d060-4f14-aaa5-9ff8157a2c45	mscameraproxy	9
bc31	a95fadb3-7f33-4158-9533-0c593afb21cc	mscameraproxy	9
99f9	ea624238-4ef8-45a9-a92b-12cc533ea2c0	ir_agent.exe	8
99f9	bfede226-c81f-43ac-a8a6-00534cc95262	ir_agent.exe	8
99f9	bfede226-c81f-43ac-a8a6-00534cc95262	chrome.exe	8
99f9	dff9bcd6-45bc-4d3e-aaf2-268cc04e50dc	ir_agent.exe	8
bc31	b7e5d8d8-d060-4f14-aaa5-9ff8157a2c45	preprocessor	8
4999	c6b8b32d-2ece-45be-9d09-12bb4789204f	ir_agent.exe	8
99f9	d19161c4-5fb7-49a6-a032-283f2a9cb95b	ir_agent.exe	7
99f9	bfede226-c81f-43ac-a8a6-00534cc95262	razer synapse 3.exe	7
99f9	d19161c4-5fb7-49a6-a032-283f2a9cb95b	dropbox.exe	7
99f9	ea624238-4ef8-45a9-a92b-12cc533ea2c0	chrome.exe	7
99f9	bfede226-c81f-43ac-a8a6-00534cc95262	razer synapse service process.exe	7
0121	84ada00d-b45f-432f-b66c-b8c450484d93	chrome.exe	7
0121	84ada00d-b45f-432f-b66c-b8c450484d93	dashlaneplugin.exe	7
0121	0f5a2f92-ca08-4860-9c11-2ddfa5aafc63	firefox.exe	7

Securing Hosts

- Microsegmentation
- Port blocking
- Separation of concerns

Securing Apps Across Hosts

- Segmentation by domain
- Targeted policies

Securing Apps

- Microsegmentation
- Port blocking

A Continuous Process

- Gather, Measure, Improve, Repeat
- Not a one-time event ☹
- Measure risk, implement targeted restrictions, measure improvement
- With the (increasingly) correct policies

Confounders

- Docker and other containerization
- Virtual machines (i.e. virtualized hardware running an OS, etc.)
- Virtual machines
- Java
- Python
- Many others

Example: What happens after one iteration?

Overexposure (one app)

site	before	after	improvement
0121	7271.854	6230.854	14.32%
28be	13	6	53.85%
3ebb	**3191.634**	**59.634**	**98.13%**
4999	40.99	34.872	14.92%
6654	70.5	64.5	8.51%
7f1c	28.75	22.75	20.87%
99f9	590.922	542.322	8.22%
9b04	73.333	65.333	10.91%
bc31	200.833	193.833	3.49%
bd92	1687.945	1676.945	0.65%
c742	7683.23	5083.23	33.84%
cbe7	496.74	415.728	16.31%
f368	2684.25	2669.417	0.55%

Complexity (one app)

site	before	after	improvement
0121	3474.058	3473.122	0.03%
28be	11.228	10.292	8.33%
3ebb	70.174	69.238	1.33%
4999	57.074	56.139	1.64%
6654	48.654	47.718	1.92%
7f1c	19.649	18.713	4.76%
99f9	1199.5	1198.564	0.08%
9b04	102.921	101.986	0.91%
bc31	369.581	368.645	0.25%
bd92	10713.16	10712.224	0.01%
c742	2153.86	2152.924	0.04%
cbe7	228.298	227.362	0.41%
f368	5572.714	5571.779	0.02%
f97a	**1.871**	**0.936**	**50.00%**

Minimize Overexposure & Complexity

- And maybe other statistics, too
- Measuring risk & insecurity
- Make and use tools

Where we've been

- Defined and use two statistics
  - Overexposure
  - Complexity
- Looked at netflow and app data from 15 sites
- Measure, optimize, repeat

The End

An updated version of these slides can be downloaded from:

https://github.com/EdgewiseNetworks/statistical-analysis-network-exposure