

Actividad de intranet

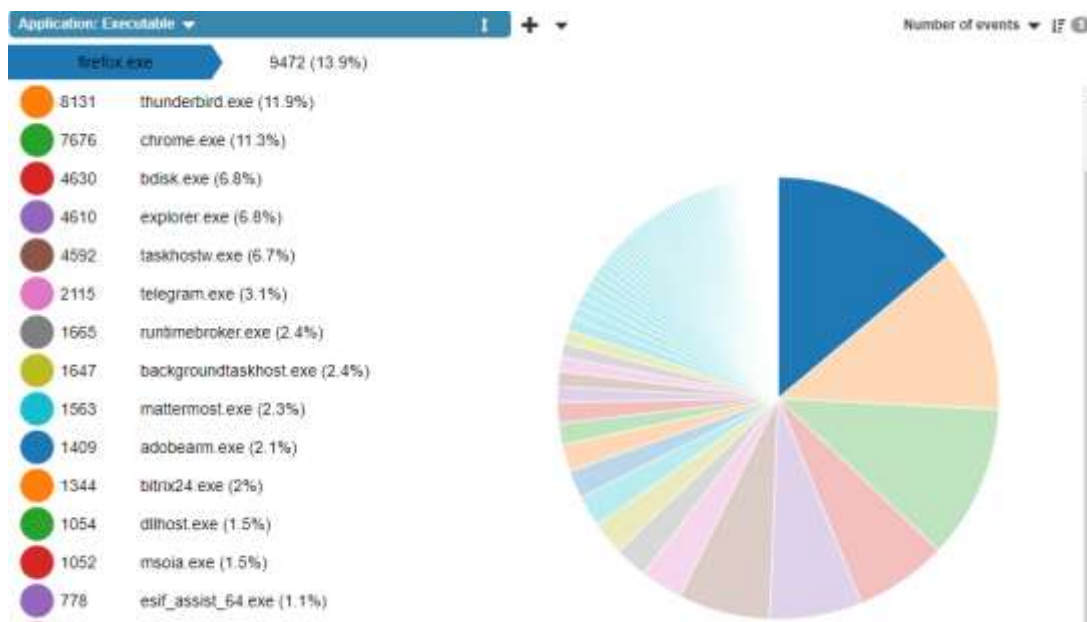
StaffCop puede obtener información sobre las conexiones de red, con criterios de evaluación como IP y puertos. Esta capacidad puede ser útil para los administradores del sistema en caso de que la política corporativa tenga una especificación para usar ciertos puertos. Las conexiones FTP se rastrean con la capacidad de ver los archivos enviados / recibidos. Se monitorea la actividad en los almacenamientos en la nube (por ejemplo, Google Drive).

StaffCop muestra la siguiente información

- Conexiones a ciertas direcciones IP
- Uso de puertos
- Uso de protocolos (https, http)
- Conexiones FTP
- Conexiones a almacenamientos en la nube
- Conexiones wifi (con bloqueos)

Uso de puertos

Por ejemplo, debemos comprender qué puertos utilizan cada aplicación y verificar si todos están permitidos por la política corporativa. El gráfico presentado en la captura de pantalla a continuación nos mostrará la participación de cada aplicación en la cantidad total de uso de los puertos.










Uso de protocolos

StaffCop rastrea el tráfico enviado / recibido a través de conexiones https encriptadas. Podemos ver qué sitios web se visitaron a través del protocolo https encriptado, y si alguno de ellos parece dudoso, podemos ver todos los detalles de las visitas a la web haciendo clic en el elemento correspondiente del gráfico circular (consulte el [seguimiento del sitio web](#) para obtener más información).

Website: Protocol	Website: Domain	Number of events	
http	staffcop.ru	712	
http	atomsecurity.com	520	
http	staffcop.su	231	
https	whatsapp.com	156	
https	yandex.ru	96	
https	staffcop.ru	60	
https	duckduckgo.com	56	
https	192.168.1.188	50	
https	atomsecurity.com	41	
https	my-cloud.pro	25	
https	google.com	25	
http	192.168.3.187	24	
https	youtube.com	23	
https	192.168.1.105	20	
https	microsoft.com	19	

Conexiones FTP

Con StaffCop puede rastrear conexiones FTP, incluida información sobre la dirección IP, el par de inicio de sesión / contraseña y las aplicaciones utilizadas para la conexión. En caso de que la opción de copia de sombra esté habilitada, StaffCop permite ver todos los archivos enviados / recibidos a través de FTP.

Time 	Type	Computer	Application	Event
2019-12-05 09:51	 FTP	DemoZoneVM1 ( firefox.exe	Login: anonymous Password: Host: 89.208.140.18
2019-09-18 16:20	 FTP	Win10NOD (1.72)	 filezilla.exe	Login: anonymous Password: anonymous@example.com Host: 91.122.30.115
2019-09-17 11:05	 FTP	Win10KES (1.24)	 filezilla.exe	Login: anonymous Password: anonymous@example.com Host: 213.180.204.183

```
Time 2019-09-17 11:05:23
Application  filezilla.exe
Event  FTP
Agent Win10KES (1.24)
Account user
Content Login: anonymous Password: anonymous@example.com Host: 213.180.204.183
PID 2392
```

Almacenamiento en la nube


Con StaffCop puede rastrear conexiones a almacenamientos en la nube (por ejemplo, Google Drive), así como a sus discos de red corporativos. Si la opción de copia de sombra está habilitada, podrá ver los archivos cargados en los almacenes en la nube.


Time	Type	Computer	Application	Event
2020-02-18 20:14:52	<input checked="" type="checkbox"/> User activity	NB0202	firefox.exe	Search portals comp0049_180220.zip - Google Диск - Mozilla Firefox https://drive.google.com/file/d/1yqoB4-Zgya_4nYFeodfEDenMfHyCtbH2/view
2020-02-18 20:14:52	<input checked="" type="checkbox"/> User activity	NB0202	firefox.exe	Search portals comp0049_180220.zip - Google Диск - Mozilla Firefox https://drive.google.com/file/d/1yqoB4-Zgya_4nYFeodfEDenMfHyCtbH2/view
2020-02-18 20:14:52	<input checked="" type="checkbox"/> User activity	NB0202	firefox.exe	Search portals Zip, UnZip - Mozilla Firefox https://drive.google.com/file/d/1yqoB4-Zgya_4nYFeodfEDenMfHyCtbH2/view
2020-02-18 20:14:52	<input checked="" type="checkbox"/> User activity	NB0202	firefox.exe	Search portals ZIP экстрактор - Mozilla Firefox

Time	2020-02-18 20:14:52
Application	firefox.exe
Filter	Search portals
Event	<input checked="" type="checkbox"/> User activity
Agent	NB0202
Account	user
Website visit	https://drive.google.com/file/d/1yqoB4-Zgya_4nYFeodfEDenMfHyCtbH2/view
Domain	google.com
Website	drive.google.com
Title	comp0049_180220.zip - Google Диск - Mozilla Firefox
Duration	00:00:01
Content	https://drive.google.com/file/d/1yqoB4-Zgya_4nYFeodfEDenMfHyCtbH2/view
PID	11496

Conexiones wifi

StaffCop le mostrará la conexión Wi-Fi con SSID (nombre de la red). Las redes Wi-Fi pueden bloquearse en base a listas blancas y negras. Es útil en caso de que a los empleados se les permita usar solo redes corporativas debido a problemas de seguridad.

Time 	Computer	Event
2020-02-26 11:56:55	NB0202	ATOM

```
Time 2020-02-26 11:56:55
Event  Wi-Fi connection
Agent NB0202
Content ATOM
```

Wi-Fi networks

Connection to Wi-Fi network

Rules: Wi-Fi networks

Allow or block all of Wi-Fi networks from list
If allow list contain Wi-Fi names, only them will be allowed to connect

