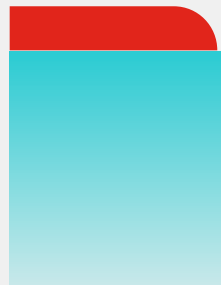


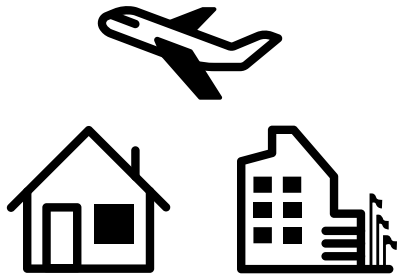
**FORTINET**<sup>®</sup>

# Fortinet Security Fabric Cybersecurity Mesh Platform

**Aigars Leončiks**  
Fortinet systems engineer Baltics



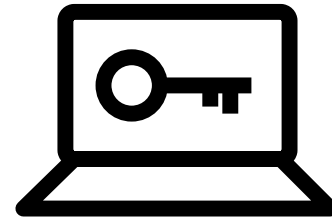
# Customer Trends



## Enabling Work From Anywhere

“The shift to remote work is expected to persist even after the pandemic. **52% of CIOs expect work from home to increase in 2021**”

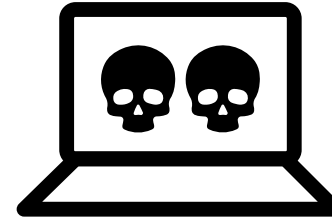
Gartner – Top Priorities for IT: Leadership Vision for 2021



## Securing Digital Acceleration

“**69% of boards have responded to COVID-19 with digital business acceleration**, while 60% have chosen improving operational excellence through digital business”

Gartner – Top Priorities for IT: Leadership Vision for 2021



## Preventing Cyber Attacks

**36% organizations state the growing sophistication of the threat landscape** is the top challenge in preventing ransomware attacks.

Fortinet – Ransomware survey 2021



## Cybersecurity Skills Shortage

**73% of organizations had at least one intrusion/breach** over the past year that can be partially attributed to a gap in cybersecurity skills

Fortinet – Cybersecurity Skills Survey 2,500 US and Canadian companies 2021

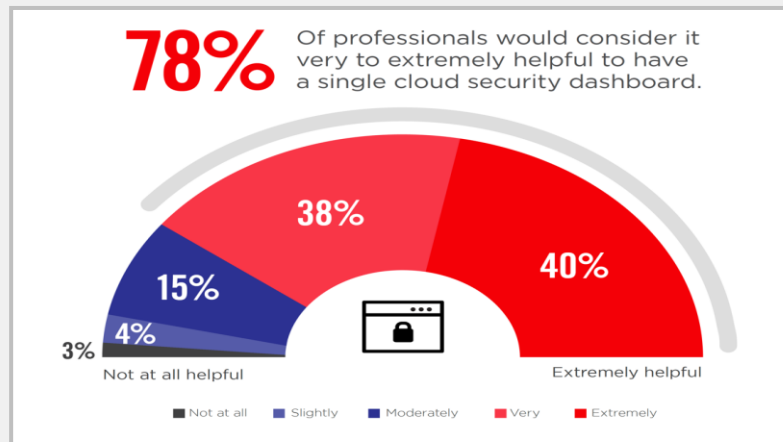
# Voice of the Customer

A ubiquitous desire for consolidation, interoperability, and automation

## What Enterprises are saying...



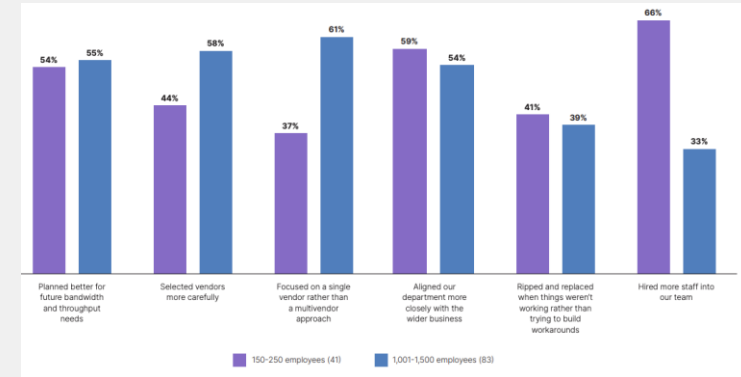
Lack of visibility, control, and staff/expertise are the top barriers to faster cloud adoption.



Desire for a single cloud security platform for consistent security policy across all cloud environments

<https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-cybersecurity-cloud-security-report-fortinet-2.5.pdf>

## What SMBs are saying...



"Lack of simple interoperability and automation between security products" is the #1 thing holding security back – according to companies with less than 500 employees...

61% of companies 1000-1500 admit in hindsight if they had to do it over again, they would have gone with a single vendor strategy

[https://www.fortinet.com/content/dam/maindam/PUBLIC/02\\_MARKETING/02\\_Collateral/eBooks/ebook-avoiding-complexity-smb.pdf](https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/02_Collateral/eBooks/ebook-avoiding-complexity-smb.pdf)



**Total Detections**

**18M**



**FortiGuard Security Services**

FortiGuard IPS Provides the latest defenses against stealthy network-level threats. It uses a customizable database of more than 11000 known threats to enable FortiGate and FortiWiFi appliances to stop attacks that evade conventional firewall defenses.

Signature Name	Volume
DNS.PTR.Records.Scan	15,628,393
MS.Windows.Workstation.Service.DoS	442,655
WordPress.xmlRpc.php.system.multicall.Amplification.Attack	389,351
Spring.Security.RegexRequestMatcher.Authentication.Bypass	187,842
NTP.Zero.Transmit.Timestamp	110,165
MS.Office.Word.Double.Free.Memory.Corruption	100,814
Web.Server.Password.Files.Access	95,653
ZGrab.Scanner	87,480
PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	78,713
TrueOnline.ZyXEL.P660HN.V1.Unauthenticated.Command.Injection	58,163
OpenVAS.Web.Scanner	56,895
HTTP.URI.SQL.Injection	55,639
Dasan.GPON.Remote.Code.Execution	54,140
Censys.io.Scanner	48,976
JAWS.DVR.CCTV.Shell.Unauthenticated.Command.Execution	40,272
Nmap.Script.Scanner	38,538
Apache.Log4j.Error.Log.Remote.Code.Execution	38,350
MS.Windows.TCP.Window.Size.Zero.DoS	35,343
MS.Windows.CVE-2020-1381.Privilege.Elevation	32,756
ThinkPHP.Controller.Parameter.Remote.Code.Execution	31,986
<b>Total</b>	<b>17,911,338</b>



**Log4Shell**

**38K**



**DoublePulsar**

**30K**



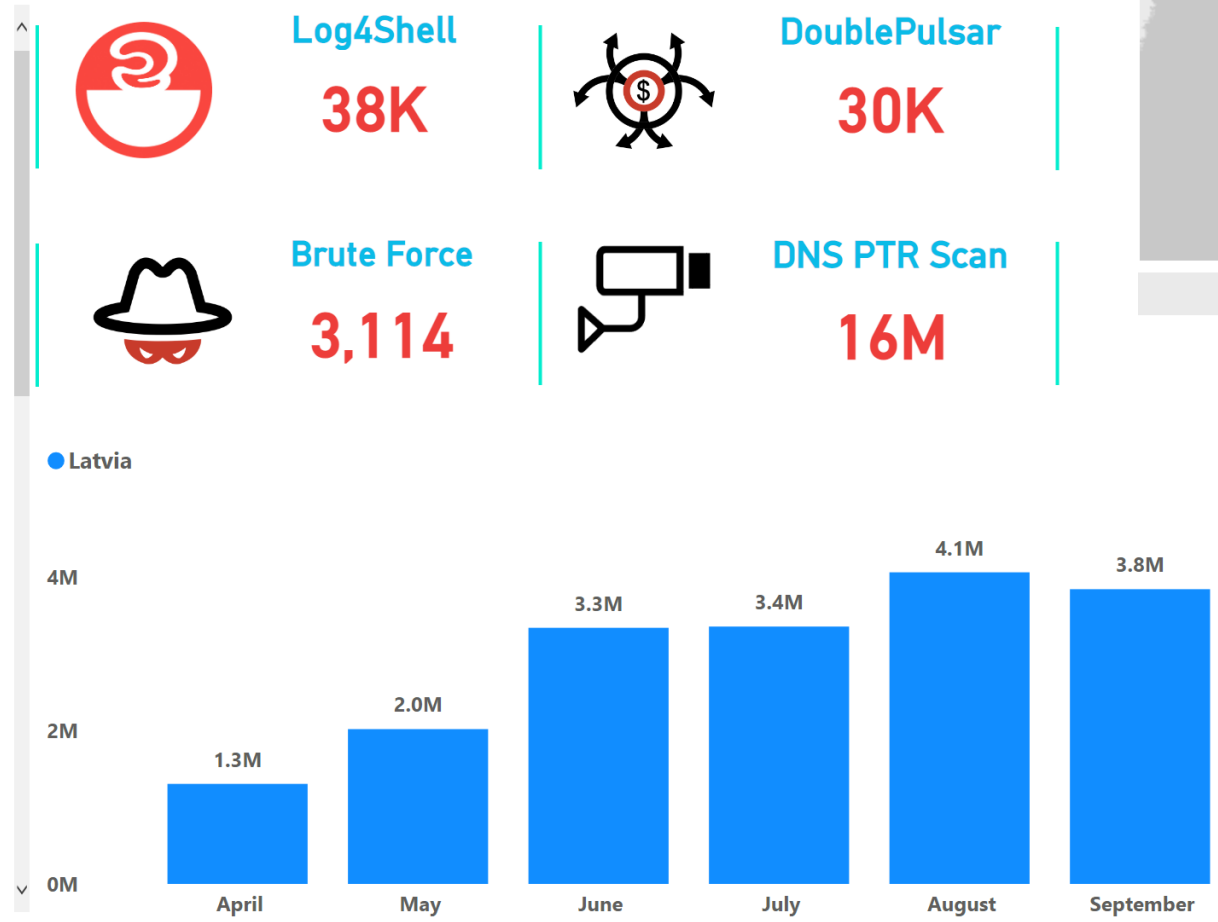
**Brute Force**

**3,114**



**DNS PTR Scan**

**16M**



**Global Threats**

Detections by volume



**Additional Resources**



**Threat Signal Report:**  
<https://www.fortiguards.com/threat-signal-report>

**Outbreak Alert:**  
<https://www.fortiguards.com/outbreak-alert>

**PSIRT Advisories:**  
<https://www.fortiguards.com/psirt>

**Zero Day Research:**  
<https://www.fortiguards.com/zeroday>



**Total Detections**

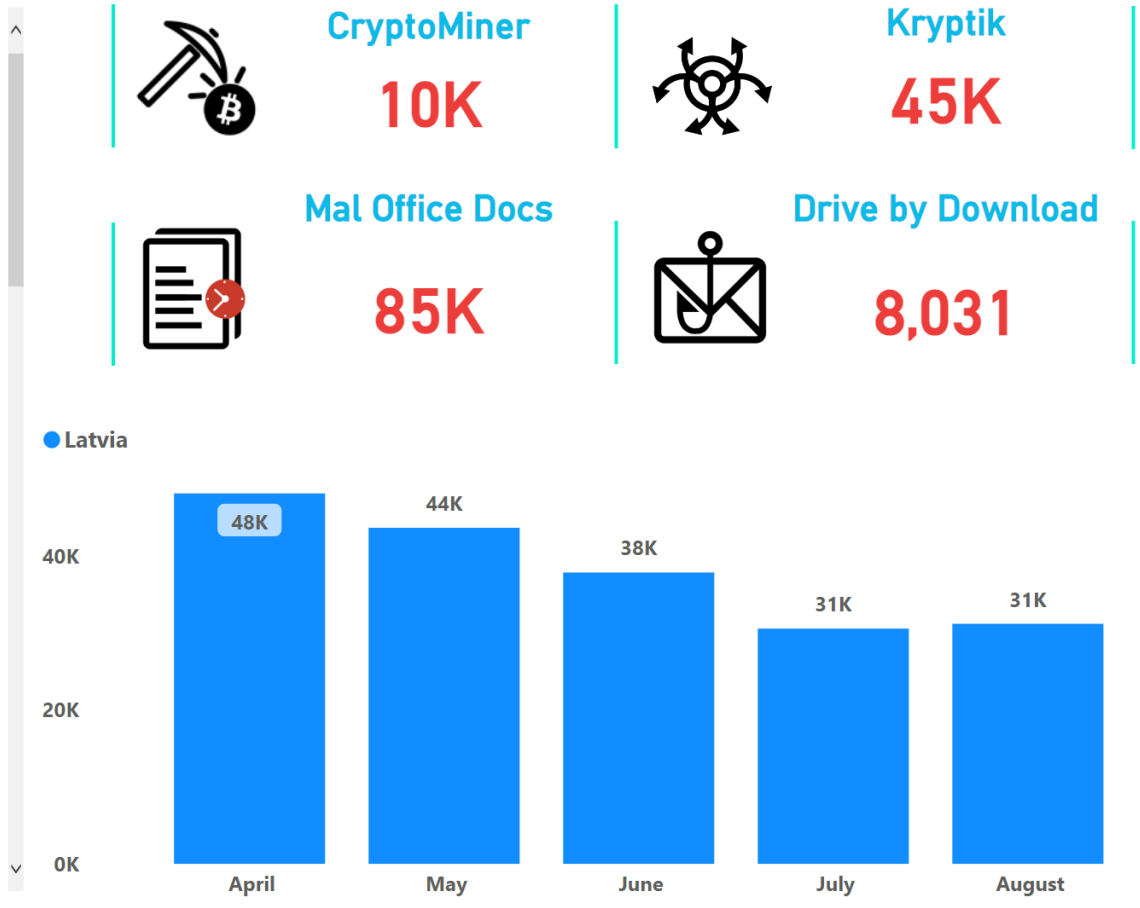
**214K**



**FortiGuard Security Services**

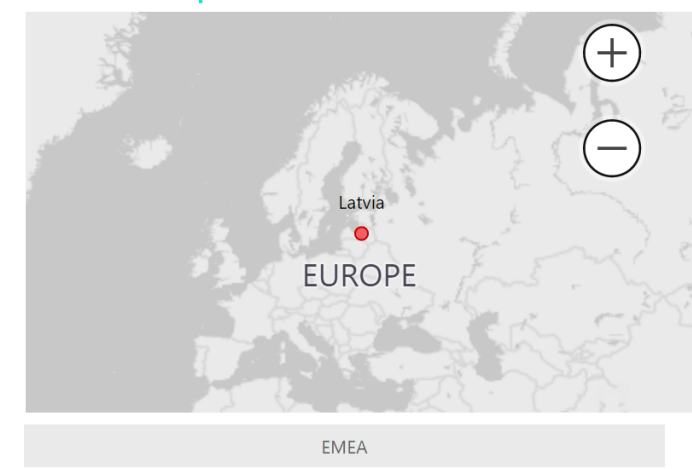
**FortiGuard Antivirus** delivers automated updates that protect against the latest polymorphing attack components, viruses, spyware, and other content-level threats. It uses industry-leading advanced detection engines to prevent both new and evolving threats from gaining a foothold inside your network, endpoint and clouds and access invaluable content.

Signature Name	Volume
MSEXcel/CVE_2017_11882!exploit	19,953
Riskware/uTorrent.E6A1	19,601
MSEXcel/CVE_2017_11882.F!exploit	13,857
MSIL/Kryptik.HLS!tr	13,399
MSEXcel/Kryptik.E!tr	10,146
MSEXcel/Agent.LA!tr	10,022
XF/Agent.BAA!tr.dldr	9,961
XF/CoinMiner.398D!tr	8,764
W32/Injector.EQPQ!tr	8,558
W32/Delf.DIB!tr.dldr	8,366
W32/Inject.XZY!tr	7,620
MSEXcel/Agent.DAC!tr	5,524
MSEXcel/CVE_2018_0798.F!exploit	5,374
MSOffice/CVE_2017_0199.536C!tr	5,176
PDF/Phish.A55D!tr	4,746
MSEXcel/Agent.4068!tr.dldr	4,634
MSEXcel/Agent.DAS!tr	4,556
MSIL/Kryptik.IY!tr	3,280
MSIL/Kryptik.TEC!tr	3,091
MSIL/Kryptik.AECU!tr	2,821
<b>Total</b>	<b>214,286</b>



**Global Threats**

Detections by volume



**Additional Resources**

**Threat Signal Report:**  
<https://www.fortiguard.com/threat-signal-report>

**Outbreak Alert:**  
<https://www.fortiguard.com/outbreak-alert>

**PSIRT Advisories:**  
<https://www.fortiguard.com/psirt>

**Zero Day Research:**  
<https://www.fortiguard.com/zeroday>



Detections by volume

Total Detections

100K



**FortiGuard Anti-Botnet Services**

The FortiGuard IP Reputation Service aggregates malicious source IP data from the Fortinet distributed network of threat sensors, CERTs, MITRE, cooperative competitors, and other global sources that collaborate to provide up-to-date threat intelligence about hostile sources.

Signature Name	Volume
Mirai.Botnet	64,664
Torpig.Mebroot.Botnet	16,101
Bladabindi.Botnet	5,485
RedLine.Stealer.Botnet	5,304
Gh0st.Rat.Botnet	5,016
Zeroaccess.Botnet	1,739
RotaJakiro.botnet	1,093
Formbook.Botnet	165
Conficker.Botnet	136
Gozi.Botnet	124
Fareit.Botnet	114
Pushdo.Botnet	66
Ganiw.Botnet	64
FrameworkPOS.Botnet	56
Xtreme.RAT.Botnet	39
RedXOR.Botnet	19
Mariposa.Botnet	14
Zeus.Botnet	12
<b>Total</b>	<b>100,256</b>



IoT- MIRAI

65K



Torpig

16K



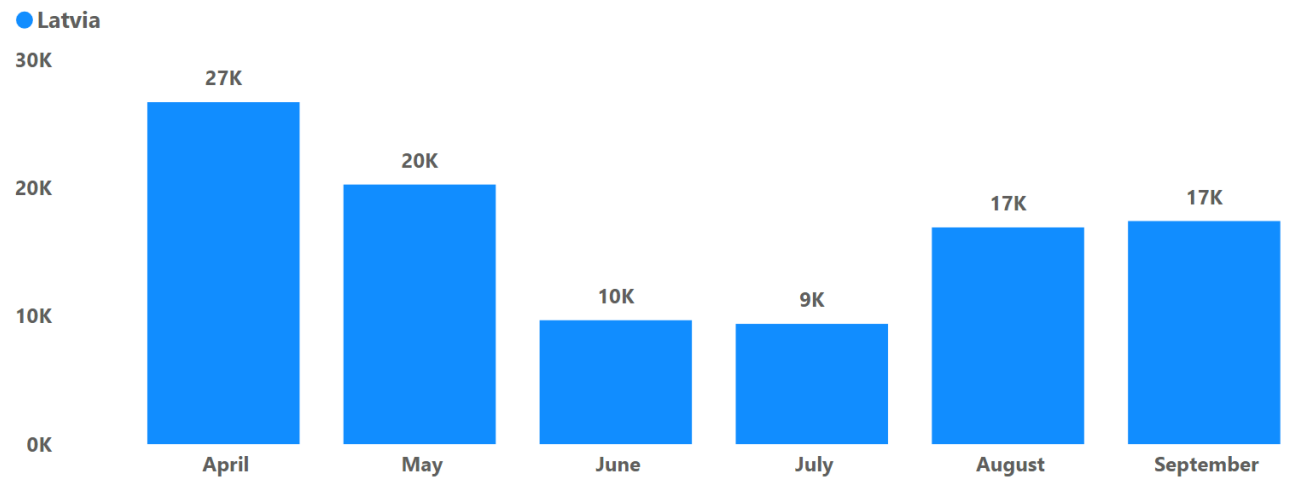
Trickbot

(Blank)



Gh0st.RAT

5,016



EMEA

**Additional Resources**



**Threat Signal Report:**  
<https://www.fortiguard.com/threat-signal-report>

**Outbreak Alert:**  
<https://www.fortiguard.com/outbreak-alert>

**PSIRT Advisories:**  
<https://www.fortiguard.com/psirt>

**Zero Day Research:**  
<https://www.fortiguard.com/zeroday>



Detections by volume

Total Detections

## 371K



### FortiGuard Endpoint vulnerability Protection

Fortinet provides a systematic and automated method of patching applications on an endpoint, eliminating manual processes while reducing the attack surface within an organization and helping meet regulatory compliance.



Signature Name	Volume
Security Vulnerability CVE-2018-1285 for log4net	38,209
Security Vulnerability CVE-2022-21426 in Oracle JRE	22,729
Security Vulnerability CVE-2022-21434 in Oracle JRE	22,724
Security Vulnerability CVE-2022-21476 in Oracle JRE	22,721
Security Vulnerability CVE-2022-21496 in Oracle JRE	22,721
Security Vulnerability CVE-2022-21443 in Oracle JRE	22,720
Multiple High and Critical Vulnerabilities Addressed in Foxit Reader before 10.1.4	8,013
Security update available in 3D Plugin Beta for Foxit Reader 10.1.4.37623	8,013
Improper Privilege Management Vulnerability CVE-22022-22782 for Windows Zoom Client	6,877
Adobe Flash Player EOL	6,863
Security Vulnerability CVE-2021-34858 for TeamViewer	6,509
Download of Code Without Integrity Check Vulnerability CVE-22022-22786 for Windows Zoom Client	5,868
Uncontrolled Search Path Element Vulnerability for Windows Zoom Client	4,412
Security Vulnerability CVE-2021-35005 for TeamViewer	4,139
Security Vulnerability CVE-2022-21248 in Oracle JRE	4,122
Security Vulnerability CVE-2022-21271 in Oracle JRE	4,122
Security Vulnerability CVE-2022-21282 in Oracle JRE	4,122
Security Vulnerability CVE-2022-21291 in Oracle JRE	4,121
Security Vulnerability CVE-2022-21296 in Oracle JRE	4,121
<b>Total</b>	<b>285,769</b>



Oracle Vulns

## 179K



Log4Net

## 38K



TeamViewer

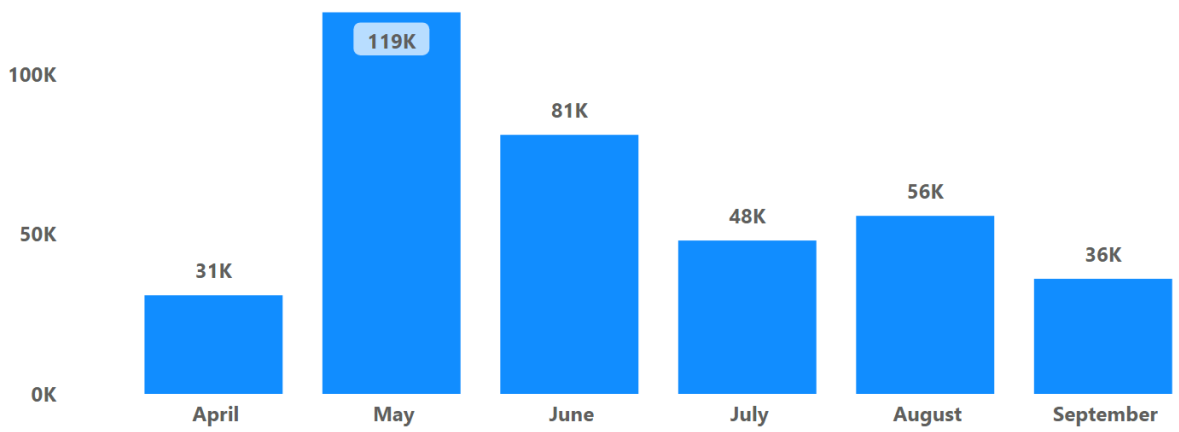
## 11K



Browser

## 8,386

Latvia



### Additional Resources



**Threat Signal Report:**  
<https://www.fortiguard.com/threat-signal-report>

**Outbreak Alert:**  
<https://www.fortiguard.com/outbreak-alert>

**PSIRT Advisories:**  
<https://www.fortiguard.com/psirt>

**Zero Day Research:**  
<https://www.fortiguard.com/zeroday>



Total Detections

**27M**



**FortiGuard Security Services**

FortiGuard IPS Provides the latest defenses against stealthy network-level threats. It uses a customizable database of more than 11000 known threats to enable FortiGate and FortiWiFi appliances to stop attacks that evade conventional firewall defenses.

Signature Name	Volume
DNS.PTR.Records.Scan	5,550,879
WordPress.xmlrpc.php.system.multicall.Amplification.Attack	5,532,707
Web.Server.Password.Files.Access	4,150,375
IP.Stream.Option	2,682,281
Apache.Log4j.Error.Log.Remote.Code.Execution	954,229
Telnet.Default.Credentials	711,300
Hikvision.Product.SDK.WebLanguage.Tag.Command.Injection	705,800
UPnP.SSDP.M.Search.Anomaly	700,586
WordPress.REST.API.Username.Enumeration.Information.Disclosure	652,796
Realtek.SDK.UDPServer.Command.Execution	649,006
ThinkPHP.Controller.Parameter.Remote.Code.Execution	632,062
Nmap.Script.Scanner	442,101
Bash.Function.Definitions.Remote.Code.Execution	370,958
TrueOnline.ZyXEL.P660HN.V1.Unauthenticated.Command.Injection	235,269
HTTP.URI.SQL.Injection	227,067
MS.SQL.Server.Login.Large.Buffer.DoS	224,608
SMB.Login.Brute.Force	220,730
HTTP.URI.Script.XSS	214,382
MS.Windows.CVE-2020-1381.Privilege.Elevation	212,279
DHCPv6.Eval.stdp.PHP.Remote.Code.Execution	204,539
<b>Total</b>	<b>27,410,261</b>



**Log4Shell**

**954K**



**Telnet Default Credentials**

**711K**



**Brute Force**

**403K**



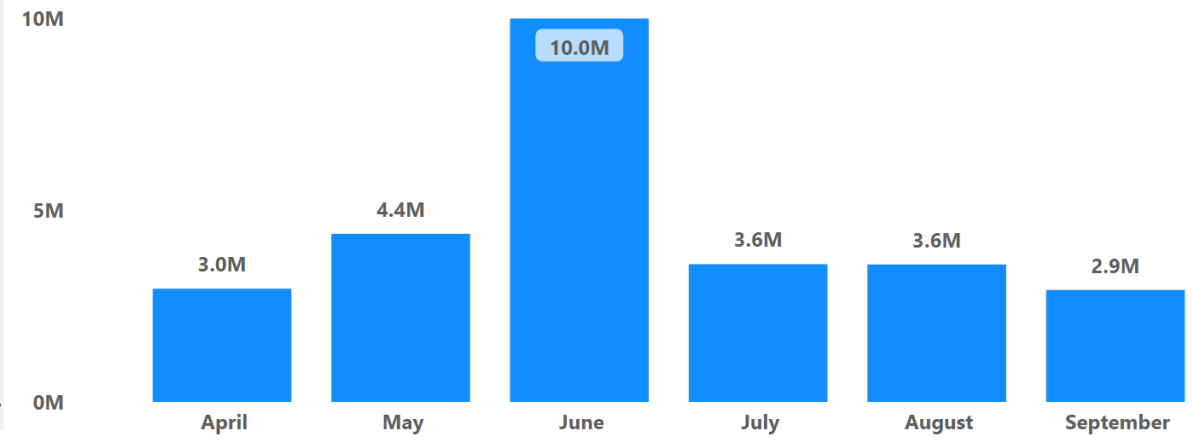
**IoT RCE**

**85K**



EMEA

● Lithuania



**Additional Resources**



**Threat Signal Report:**  
<https://www.fortiguards.com/threat-signal-report>

**Outbreak Alert:**  
<https://www.fortiguards.com/outbreak-alert>

**PSIRT Advisories:**  
<https://www.fortiguards.com/psirt>

**Zero Day Research:**  
<https://www.fortiguards.com/zeroday>





**Total Detections**

2M



**FortiGuard Security Services**

**FortiGuard Antivirus** delivers automated updates that protect against the latest polymorphing attack components, viruses, spyware, and other content-level threats. It uses industry-leading advanced detection engines to prevent both new and evolving threats from gaining a foothold inside your network, endpoint and clouds and access invaluable content.

Signature Name	Volume
Linux/CoinMiner.QN!tr.dldr	232,042
MSEXcel/CVE_2018_0798.F!exploit	216,760
MSEXcel/CVE_2017_11882.F!exploit	209,286
JS/ProxyChanger.GB!tr	141,747
NSIS/Injector.AOW!tr	87,387
Riskware/uTorrent.E6A1	65,338
Adware/Lnkr	56,605
W32/BitCoinMiner.BXPOTENTIALLYUNSAFE!tr	51,682
MSIL/Kryptik.ADNS!tr	49,654
MSIL/GenKryptik.FXHD!tr	42,528
MSEXcel/CVE_2017_11882!exploit	28,167
MSIL/GenKryptik.FWDV!tr	27,845
MSIL/GenKryptik.FSII!tr	25,087
MSIL/Kryptik.EOY!tr	24,661
Riskware/Application2	22,305
MSIL/Kryptik.AEWA!tr	21,571
VBS/Nyx.6985!tr	19,297
W32/ASH!tr	19,052
MSIL/Kryptik.AESN!tr	15,674
MSIL/GenKryptik.FKZ7!tr	15,410
<b>Total</b>	<b>1,669,612</b>



**CryptoMiner**

287K



**Kryptik**

374K



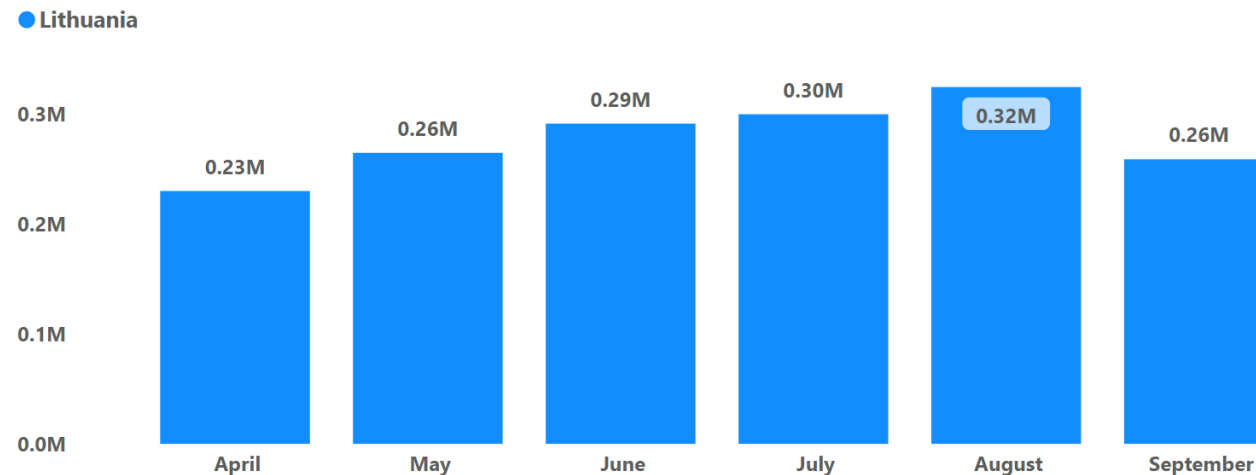
**Mal Office Docs**

460K



**Drive by Download**

48K



**Global Threats**

Detections by volume



**Additional Resources**



**Threat Signal Report:**  
<https://www.fortiguards.com/threat-signal-report>

**Outbreak Alert:**  
<https://www.fortiguards.com/outbreak-alert>

**PSIRT Advisories:**  
<https://www.fortiguards.com/psirt>

**Zero Day Research:**  
<https://www.fortiguards.com/zeroday>



Total Detections

2M



**FortiGuard Anti-Botnet Services**

The FortiGuard IP Reputation Service aggregates malicious source IP data from the Fortinet distributed network of threat sensors, CERTs, MITRE, cooperative competitors, and other global sources that collaborate to provide up-to-date threat intelligence about hostile sources.

Signature Name	Volume
Zeroaccess.Botnet	682,137
Mirai.Botnet	289,428
Necurs.Botnet	224,613
Trojan.TrickBot	216,370
Ramnit.Botnet	74,668
Sora.Botnet	69,309
Formbook.Botnet	54,060
STRRAT.Botnet	49,683
Torpig.Mebroot.Botnet	48,167
RedLine.Stealer.Botnet	34,907
Conficker.Botnet	23,348
Bladabindi.Botnet	15,652
Gh0st.Rat.Botnet	15,254
RotaJakiro.botnet	10,055
Sality.Botnet	8,305
DCRat.Botnet	5,562
Quasar.Botnet	5,226
Emotet.Cridex.Botnet	5,016
<b>Total</b>	<b>1,841,426</b>



**IoT- MIRAI**

289K



**Zero Access**

682K



**Trickbot**

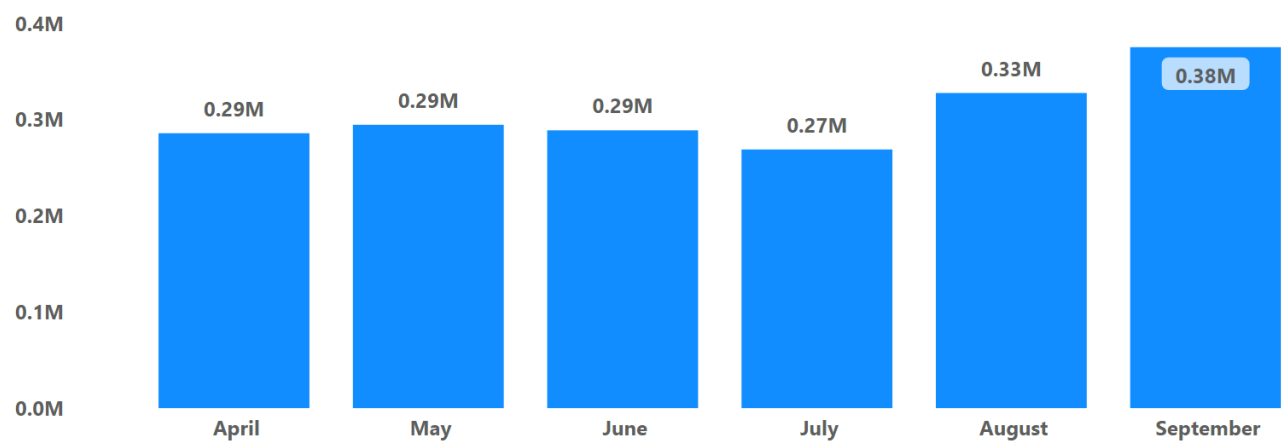
216K



**Necurs**

225K

● Lithuania



**Global Threats**

Detections by volume



EMEA

**Additional Resources**



**Threat Signal Report:**  
<https://www.fortiguards.com/threat-signal-report>

**Outbreak Alert:**  
<https://www.fortiguards.com/outbreak-alert>

**PSIRT Advisories:**  
<https://www.fortiguards.com/psirt>

**Zero Day Research:**  
<https://www.fortiguards.com/zeroday>



Detections by volume

Total Detections

**606K**



**FortiGuard Endpoint vulnerability Protection**

Fortinet provides a systematic and automated method of patching applications on an endpoint, eliminating manual processes while reducing the attack surface within an organization and helping meet regulatory compliance.



EMEA

Signature Name	Volume
Security Vulnerability CVE-2018-1285 for log4net	35,756
Security Vulnerability CVE-2021-34858 for TeamViewer	25,369
Security Vulnerability CVE-2021-35005 for TeamViewer	24,318
Security Vulnerability CVE-2022-21426 in Oracle JRE	19,373
Security Vulnerability CVE-2022-21496 in Oracle JRE	19,373
Security Vulnerability CVE-2022-21434 in Oracle JRE	19,370
Security Vulnerability CVE-2022-21476 in Oracle JRE	19,366
Security Vulnerability CVE-2022-21443 in Oracle JRE	19,365
Security Vulnerability CVE-2022-21305 in Oracle JRE	16,468
Security Vulnerability CVE-2022-21282 in Oracle JRE	16,465
Security Vulnerability CVE-2022-21293 in Oracle JRE	16,465
Security Vulnerability CVE-2022-21296 in Oracle JRE	16,465
Security Vulnerability CVE-2022-21341 in Oracle JRE	16,464
Security Vulnerability CVE-2022-21271 in Oracle JRE	16,463
Security Vulnerability CVE-2022-21291 in Oracle JRE	16,463
Security Vulnerability CVE-2022-21299 in Oracle JRE	16,463
Security Vulnerability CVE-2022-21340 in Oracle JRE	16,463
Security Vulnerability CVE-2022-21360 in Oracle JRE	16,461
Security Vulnerability CVE-2022-21294 in Oracle JRE	16,460
Security Vulnerability CVE-2022-21365 in Oracle JRE	16,459
Security Vulnerability CVE-2022-21248 in Oracle JRE	16,457
Security Vulnerability CVE-2022-21349 in Oracle JRE	16,453
Security Vulnerability CVE-2022-21540 in Oracle JRE	8,574
<b>Total</b>	<b>586,239</b>



**Oracle Vulns**

**394K**



**Log4Net**

**36K**



**TeamViewer**

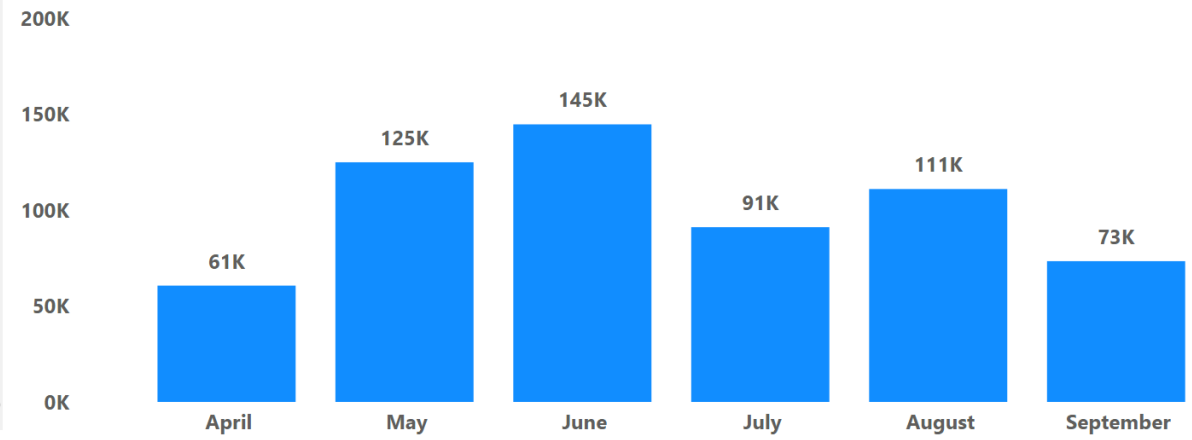
**50K**



**Browser**

**9,854**

● Lithuania



**Additional Resources**



**Threat Signal Report:**  
<https://www.fortiguards.com/threat-signal-report>

**Outbreak Alert:**  
<https://www.fortiguards.com/outbreak-alert>

**PSIRT Advisories:**  
<https://www.fortiguards.com/psirt>

**Zero Day Research:**  
<https://www.fortiguards.com/zeroday>



Total Detections

21bn



**FortiGuard Security Services**

FortiGuard IPS Provides the latest defenses against stealthy network-level threats. It uses a customizable database of more than 11000 known threats to enable FortiGate and FortiWiFi appliances to stop attacks that evade conventional firewall defenses.

Signature Name	Volume
NTP.Monlist.Command.DoS	21,366,928,345
Apache.Optionsbleed.Scanner	40,399,406
SIPVicious.svcrack.Brute.Force.Login	16,780,658
Hikvision.Product.SDK.WebLanguage.Tag.Command.Injection	14,147,624
WordPress.xmlrpc.Pingback.DoS	5,574,665
Realtek.SDK.UDP.Server.Command.Execution	4,713,219
Netcore.Netis.Devices.Hardcoded.Password.Security.By pass	3,000,157
Memcached.UDP.Amplification.Detection	2,798,958
Linux.Kernel.TCP.SACK.Panic.DoS	2,441,677
TrueOnline.ZyXEL.P660HN.V1.Unauthenticated.Command.Injection	2,214,251
Telnet.Default.Credentials	2,190,621
ThinkPHP.Controller.Parameter.Remote.Code.Execution	2,157,289
PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	890,452
Web.Server.Password.Files.Access	873,689
MySQL.Login.Brute.Force	801,408
D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	797,901
WordPress.xmlrpc.php.system.multicall.Amplification.Attack	606,931
Shenzhen.TVT.DVR.Remote.Code.Execution	441,766
<b>Total</b>	<b>21,472,496,637</b>



**Log4Shell**

289K



**DoublePulsar**

32K



**Brute Force**

18M



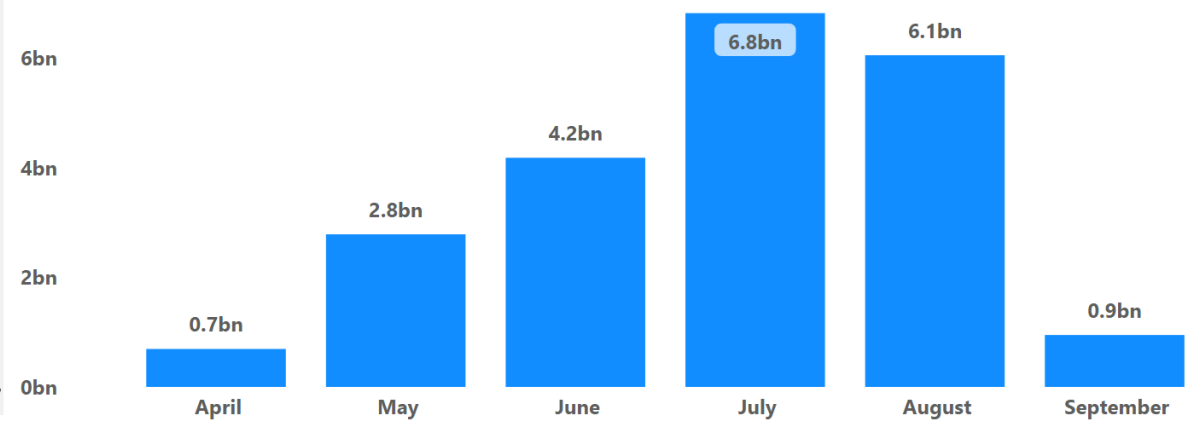
**NTP DDoS**

21bn



EMEA

● Estonia



**Additional Resources**



**Threat Signal Report:**  
<https://www.fortiguards.com/threat-signal-report>

**Outbreak Alert:**  
<https://www.fortiguards.com/outbreak-alert>

**PSIRT Advisories:**  
<https://www.fortiguards.com/psirt>

**Zero Day Research:**  
<https://www.fortiguards.com/zeroday>



Total Detections

200K



**FortiGuard Security Services**

**FortiGuard Antivirus** delivers automated updates that protect against the latest polymorphing attack components, viruses, spyware, and other content-level threats. It uses industry-leading advanced detection engines to prevent both new and evolving threats from gaining a foothold inside your network, endpoint and clouds and access invaluable content.

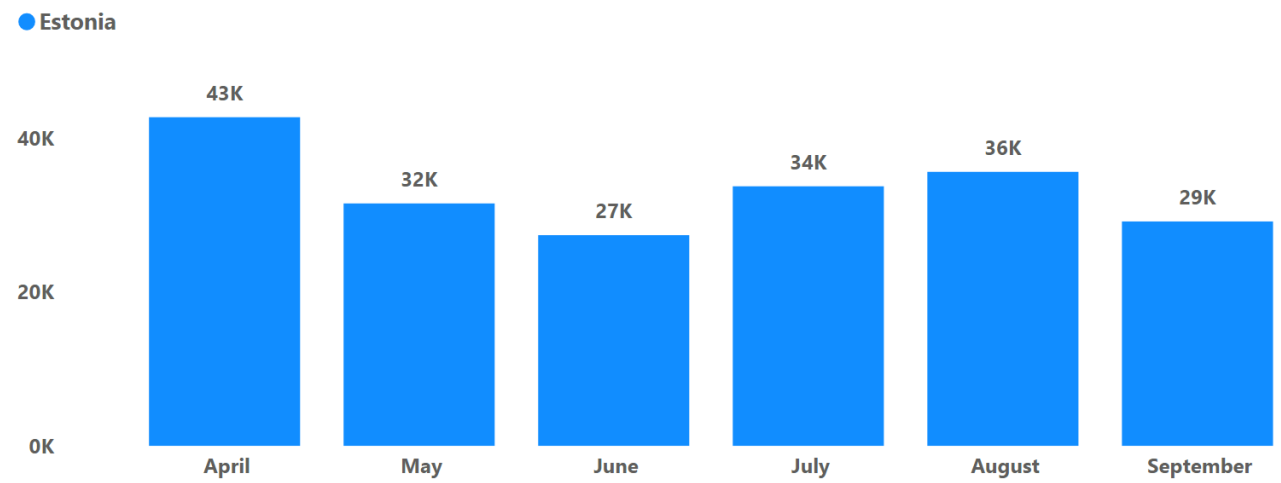
Signature Name	Volume
Riskware/BitTorrent.PUP	27,420
Riskware/Application2	18,122
Adware/Miner	16,019
Riskware/uTorrent.E6A1	15,681
Riskware/Yandex	14,051
MSEXcel/CVE_2017_11882!exploit	11,019
PowerShell/Agent.FSW!tr	9,541
Riskware/NDAoF_TNICA	8,625
NSIS/Injector.AOW!tr	6,644
VBS/Agent.VHG!tr	6,332
MSIL/GenKryptik.FXRD!tr	5,788
Riskware/Agent	5,170
JS/CoinMiner.DO!tr	4,308
HTML/Generic.31221958!tr	3,844
MSEXcel/CVE_2017_11882.F!exploit	2,862
PDF/Phishing.RUA!tr	2,278
JS/Agent.1298!tr	2,180
Adware/Lnkr	2,037
HTML/PHISHING.AAD5!tr	2,035
MSIL/Kryptik.AFAE!tr	2,010
<b>Total</b>	<b>200,119</b>

**CryptoMiner**  
**22K**

**Kryptik**  
**18K**

**Mal Office Docs**  
**15K**

**Drive by Download**  
**17K**



**Global Threats**

Detections by volume



**Additional Resources**



**Threat Signal Report:**  
<https://www.fortiguard.com/threat-signal-report>

**Outbreak Alert:**  
<https://www.fortiguard.com/outbreak-alert>

**PSIRT Advisories:**  
<https://www.fortiguard.com/psirt>

**Zero Day Research:**  
<https://www.fortiguard.com/zeroday>



Total Detections

3M



**FortiGuard Anti-Botnet Services**

The FortiGuard IP Reputation Service aggregates malicious source IP data from the Fortinet distributed network of threat sensors, CERTs, MITRE, cooperative competitors, and other global sources that collaborate to provide up-to-date threat intelligence about hostile sources.

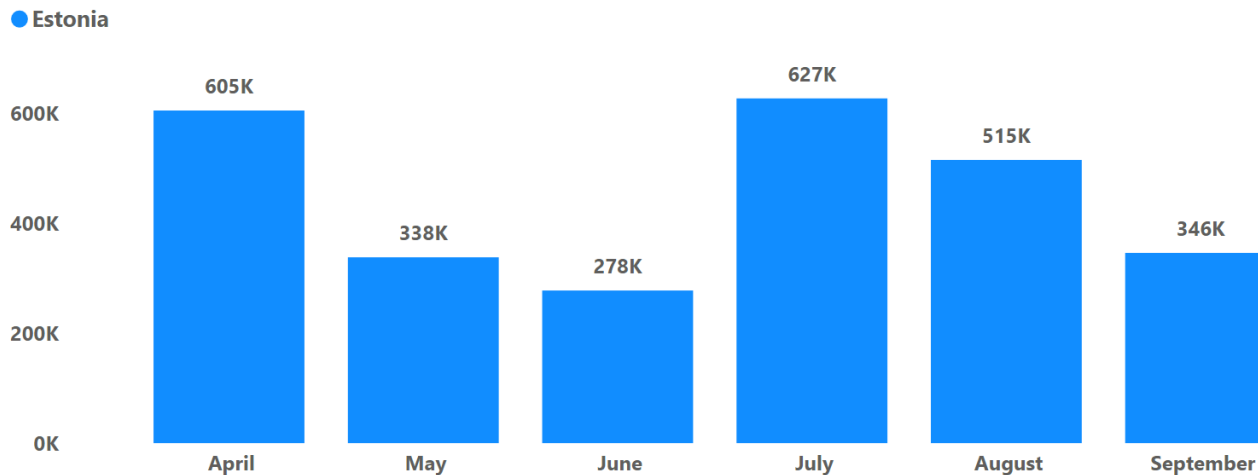
Signature Name	Volume
Zeroaccess.Botnet	1,769,679
Mirai.Botnet	390,081
Sora.Botnet	339,794
Bladabindi.Botnet	90,666
Gh0st.Rat.Botnet	80,487
RotaJakiro.botnet	9,761
Xtreme.RAT.Botnet	5,629
RedLine.Stealer.Botnet	4,427
Andromeda.Botnet	3,917
Formbook.Botnet	3,403
Hajime.Botnet	3,130
RedXOR.Botnet	2,453
Torpig.Mebrook.Botnet	1,836
Conficker.Botnet	1,579
Pushdo.Botnet	1,381
Ganiw.Botnet	575
Zeus.Botnet	429
Sality.Botnet	250
<b>Total</b>	<b>2,710,071</b>

**IoT- MIRAI**  
390K

**ZeroAccess**  
2M

**Sora**  
340K

**Bladabindi**  
91K



**Global Threats**

Detections by volume



**Additional Resources**



**Threat Signal Report:**  
<https://www.fortiguards.com/threat-signal-report>

**Outbreak Alert:**  
<https://www.fortiguards.com/outbreak-alert>

**PSIRT Advisories:**  
<https://www.fortiguards.com/psirt>

**Zero Day Research:**  
<https://www.fortiguards.com/zeroday>



Total Detections

131K



**FortiGuard Endpoint vulnerability Protection**

Fortinet provides a systematic and automated method of patching applications on an endpoint, eliminating manual processes while reducing the attack surface within an organization and helping meet regulatory compliance.

Signature Name	Volume
PostgreSQL: Multiple features escape security restricted operation sandbox	8,405
PostgreSQL: Reconnection can downgrade connection security settings	8,404
PostgreSQL: psql set allows overwriting specially treated variables	8,403
Uncontrolled Search Path Element Vulnerability CVE-2022-22943 for VMware Tools	8,351
PostgreSQL: Memory disclosure in certain queries	8,199
PostgreSQL: Windows installer runs executables from uncontrolled directories	8,199
PostgreSQL: Uncontrolled search path element in logical replication	8,174
PostgreSQL: ALTER ... DEPENDS ON EXTENSION is missing authorization checks.	8,173
Security Vulnerability CVE-2018-1285 for log4net	5,101
VideoLAN Security Bulletin VLC 3.0.13	4,537
VideoLAN Security Bulletin VLC 3.0.12	4,097
Security Vulnerability CVE-2021-34858 for TeamViewer	3,013
Security Vulnerability CVE-2021-35005 for TeamViewer	2,849
Microsoft: Windows LDAP Remote Code Execution Vulnerability	2,268
Security Vulnerability CVE-2022-21476 in Oracle JRE	1,273
Security Vulnerability CVE-2022-21434 in Oracle JRE	1,272
<b>Total</b>	<b>128,488</b>



**Oracle Vulns**

14K



**Log4Net**

5,101



**TeamViewer**

5,862



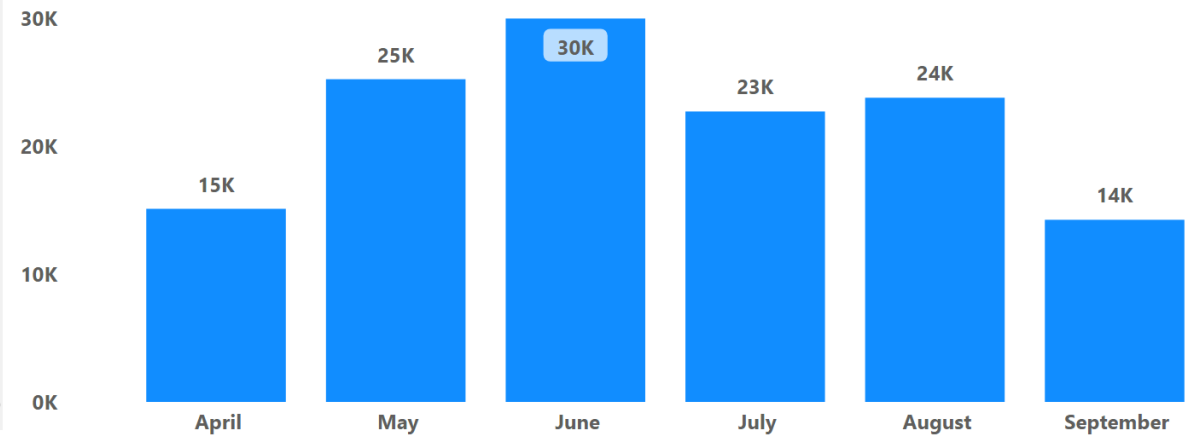
**Browser**

6,881



EMEA

● Estonia



**Additional Resources**



**Threat Signal Report:**  
<https://www.fortiguards.com/threat-signal-report>

**Outbreak Alert:**  
<https://www.fortiguards.com/outbreak-alert>

**PSIRT Advisories:**  
<https://www.fortiguards.com/psirt>

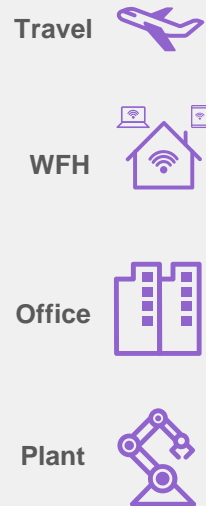
**Zero Day Research:**  
<https://www.fortiguards.com/zeroday>



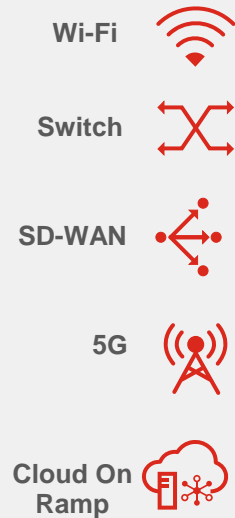
# Resulting Cybersecurity Challenges

**A lot** of challenges across **a lot** of edges that can lead to **a lot** of products, complexity, and threats

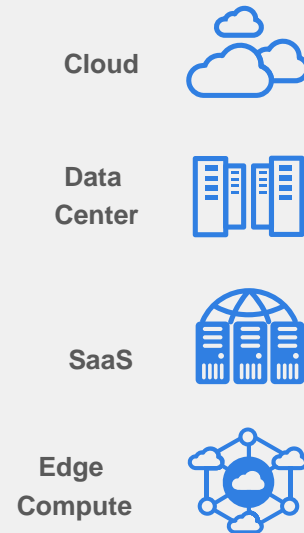
## Users & Devices



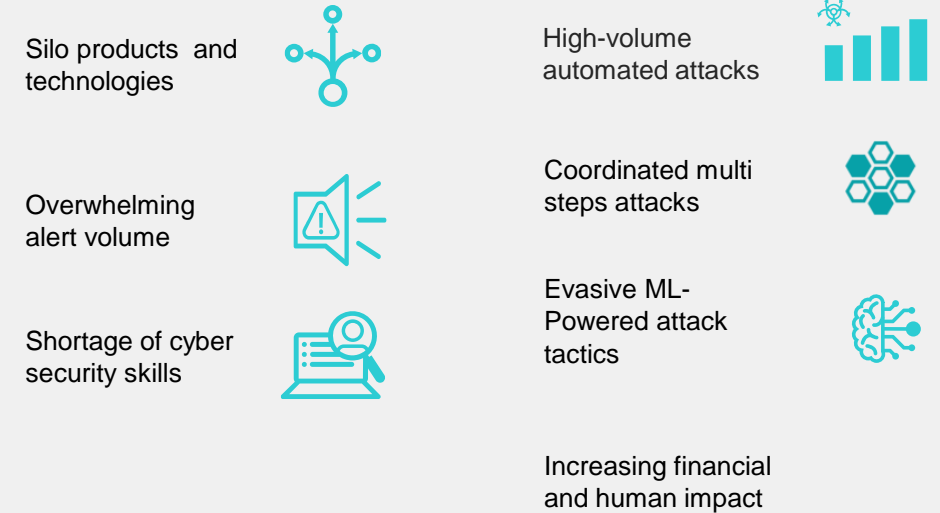
## Networks



## Applications



## SecOps



Ensuring consistent enterprise class security independent of device type & location

The Perimeter has expanded across the entire network creating more edges which need to be secured

Applications continue to move and are spread across multiple cloud creating complex operational overhead that result in security challenges

The volume of security products and information overwhelms teams chronically short of skilled staff, slowing the ability to detect and respond to incidents

Attackers will continue to innovate leveraging AI driven insights and large scale automated execution across the full attack surface and cycle

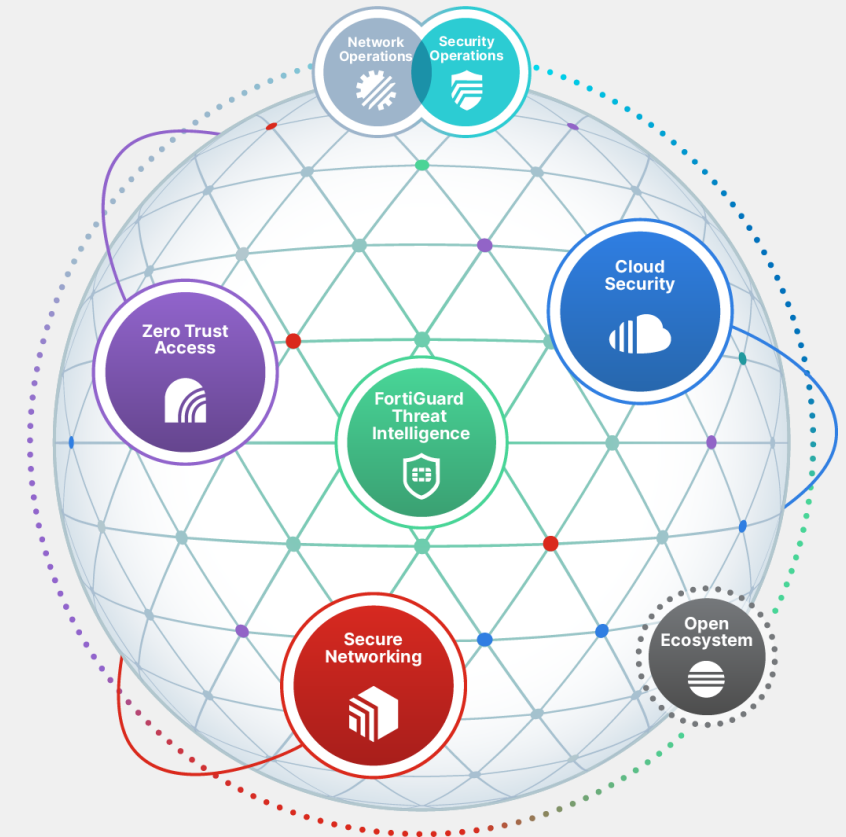
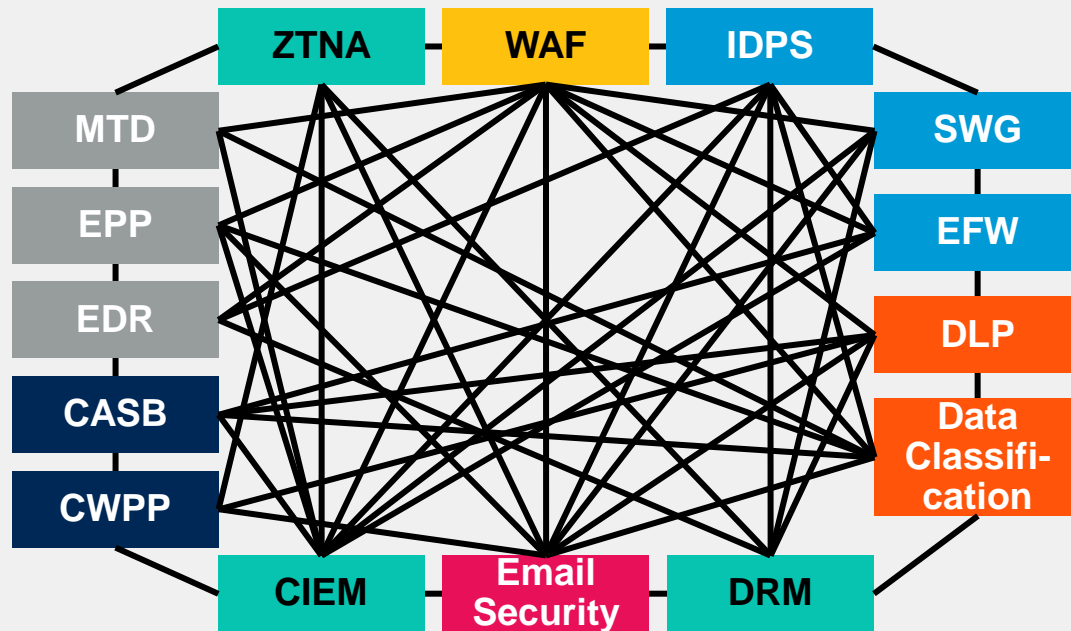




# Gartner Cybersecurity Mesh Architecture

Gartner®

FORTINET®



Executive Guide to Cybersecurity Mesh, 2022

Felix Gaetgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, Patrick Hevesi. As of October 2021

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Fortinet.

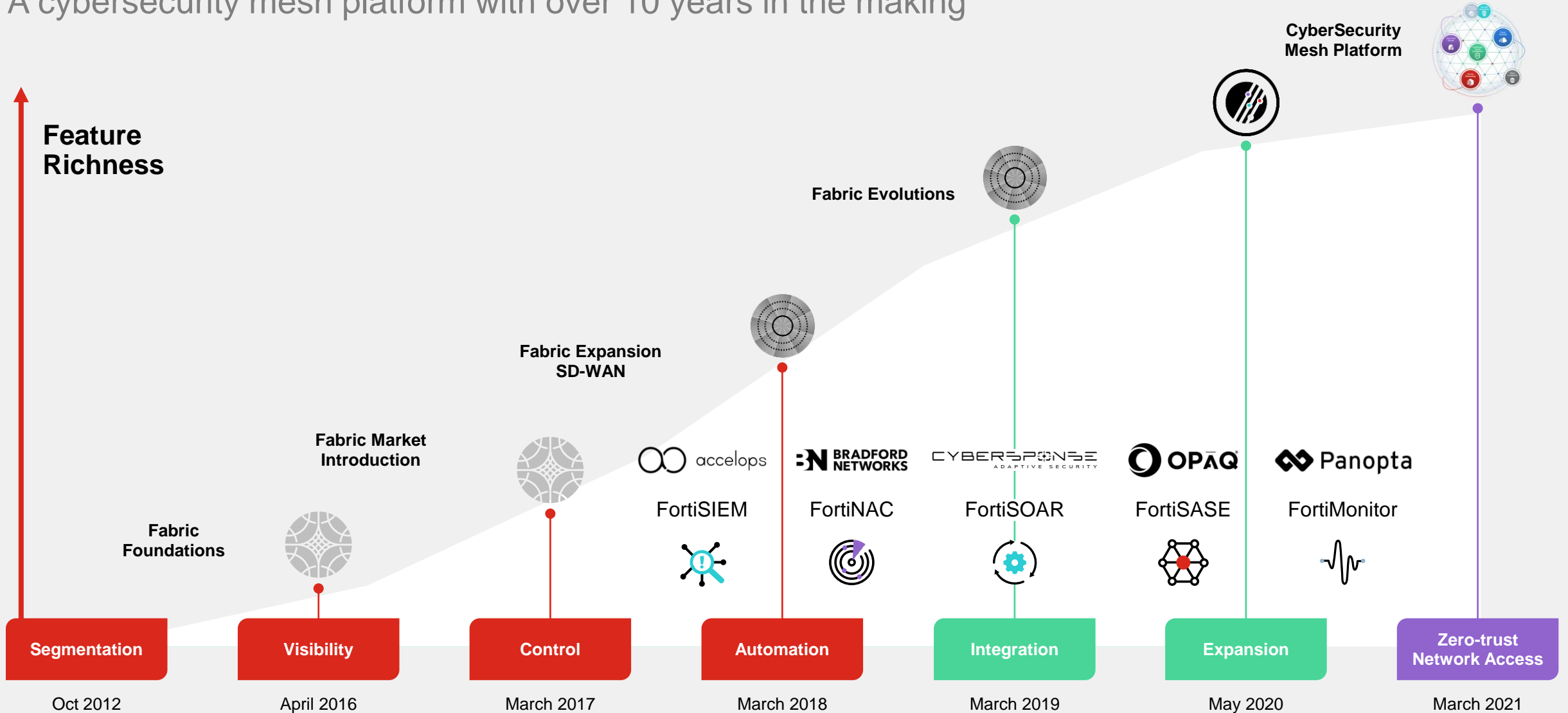


GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

© Fortinet Inc. All Rights Reserved.

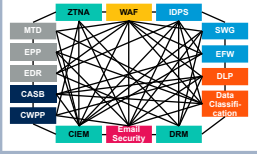
# Evolution of the Fortinet Security Fabric

A cybersecurity mesh platform with over 10 years in the making



# Fortinet PoV: Fortinet Security Fabric IS a Cybersecurity Mesh Platform

## Gartner CSMA



Identity, Access, & Content Control

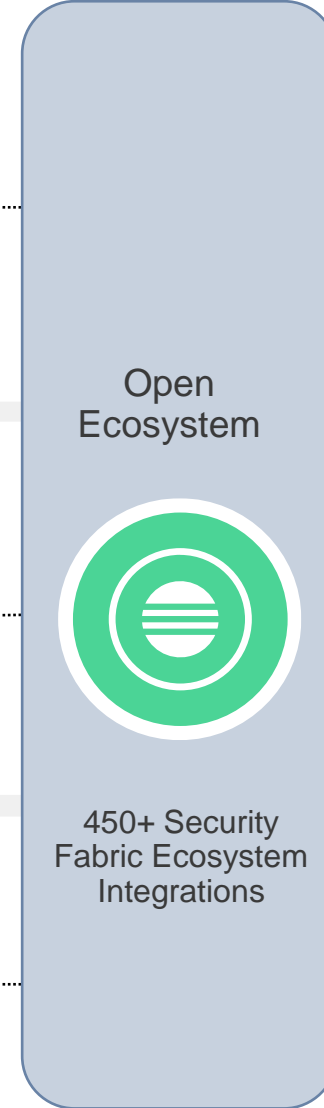
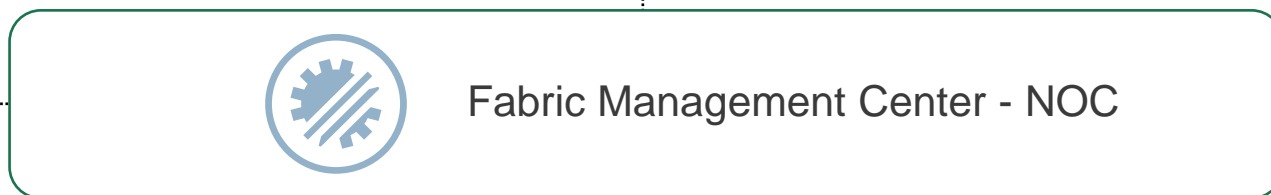
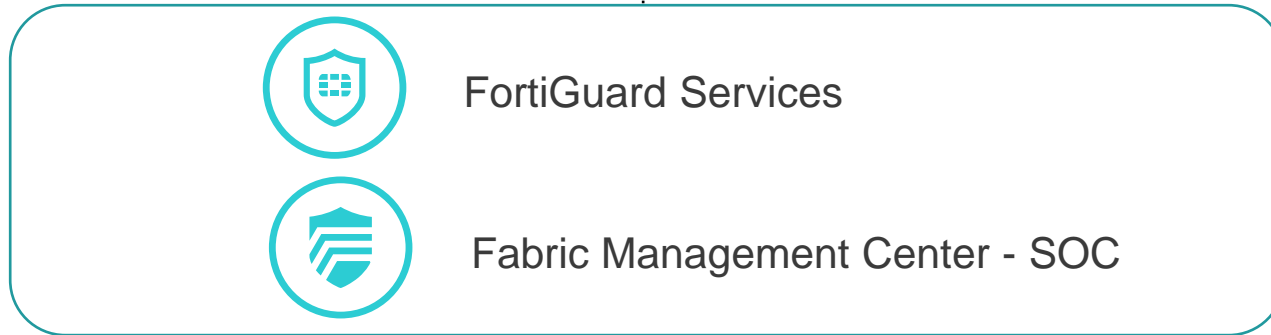
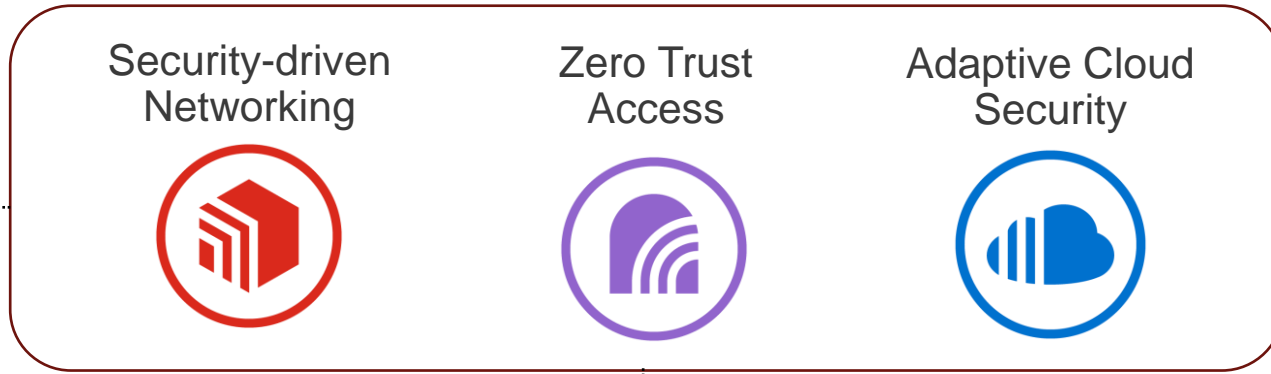
Security Intelligence, Analytics, Detection & Response

Policy Management & Orchestration, Dashboards

Executive Guide to Cybersecurity Mesh, 2022  
Felix Gaetgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, Patrick Hevesi. As of October 2021

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Fortinet.

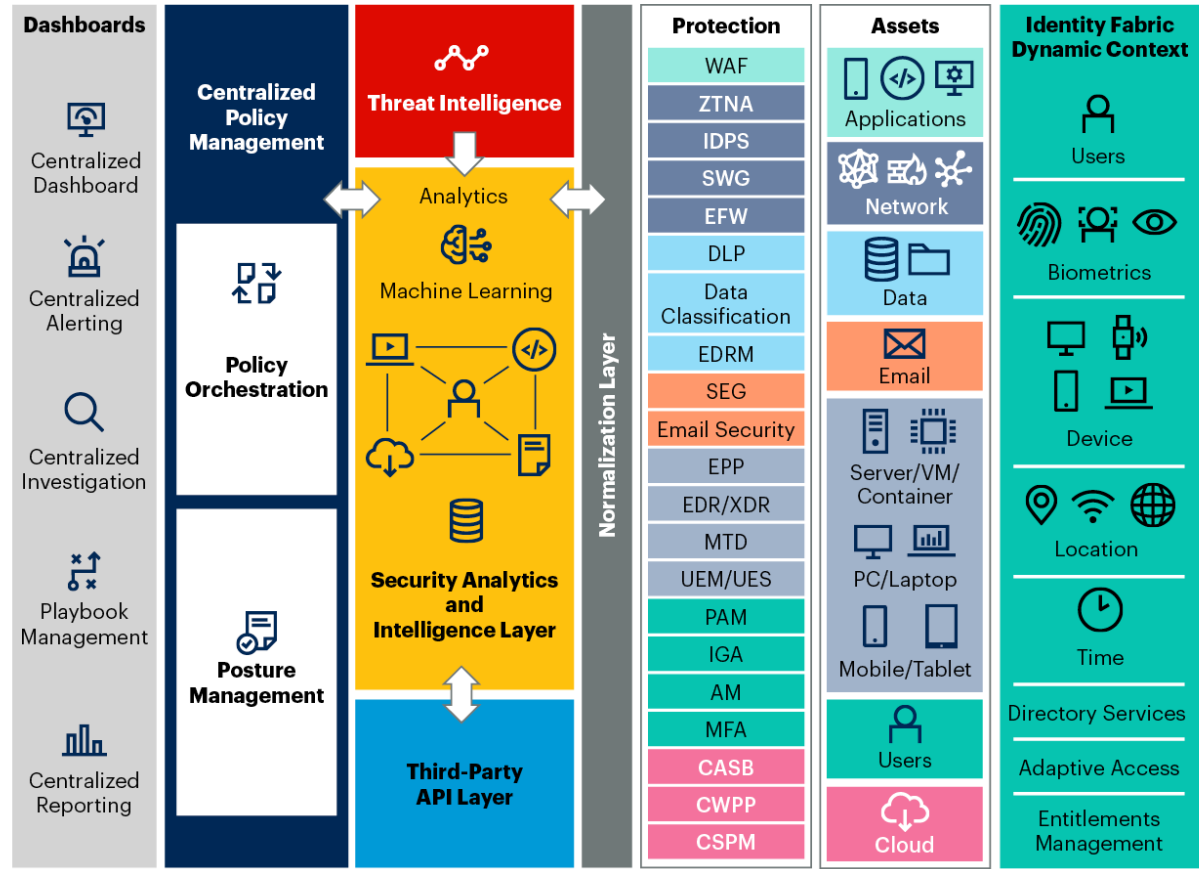
## Fortinet Security Fabric



# Fortinet Makes Cybersecurity Mesh Architecture Possible



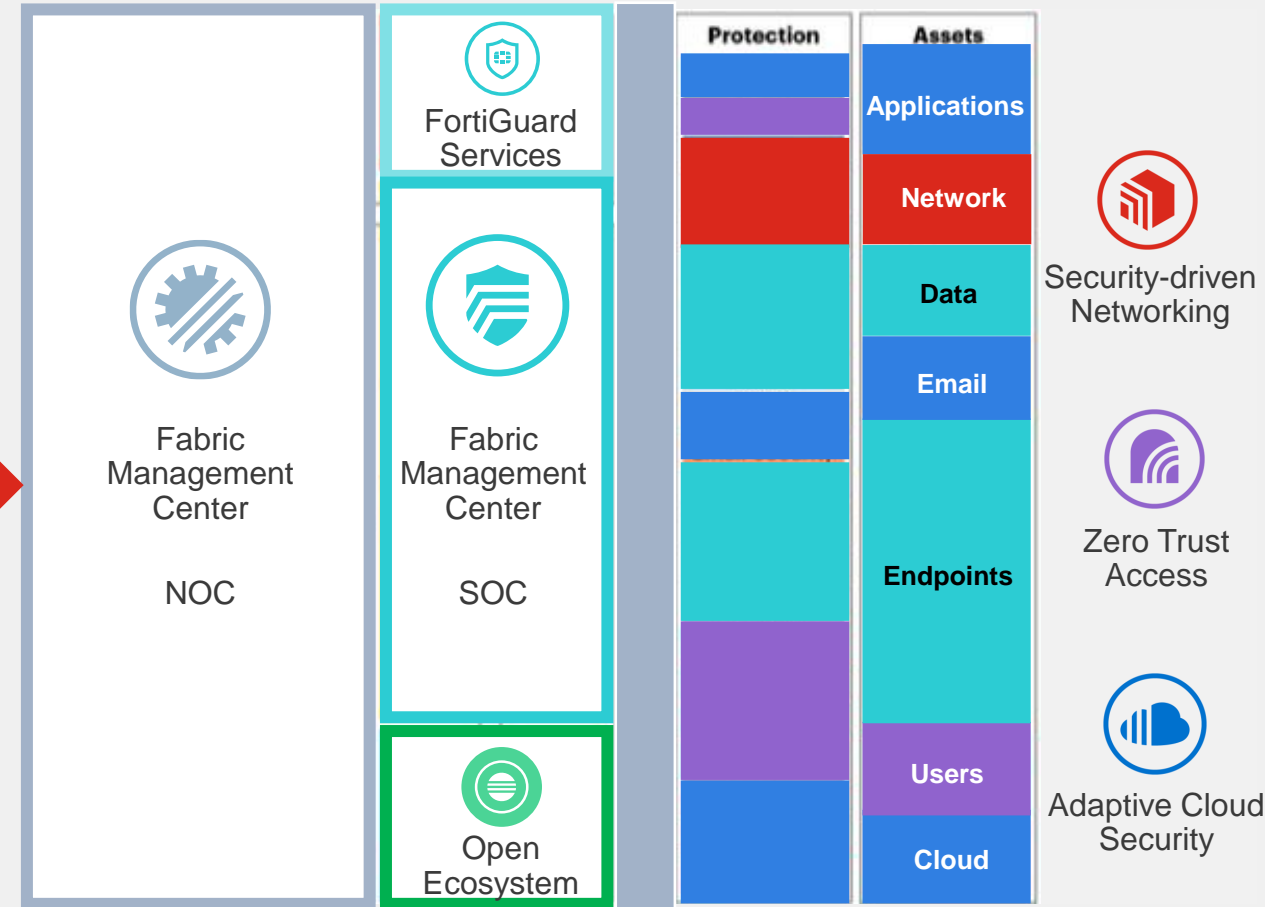
## Cybersecurity Mesh Architecture



Source: Gartner  
756156\_C



## Fortinet Security Fabric in Action



© Fortinet Inc. All Rights Reserved.



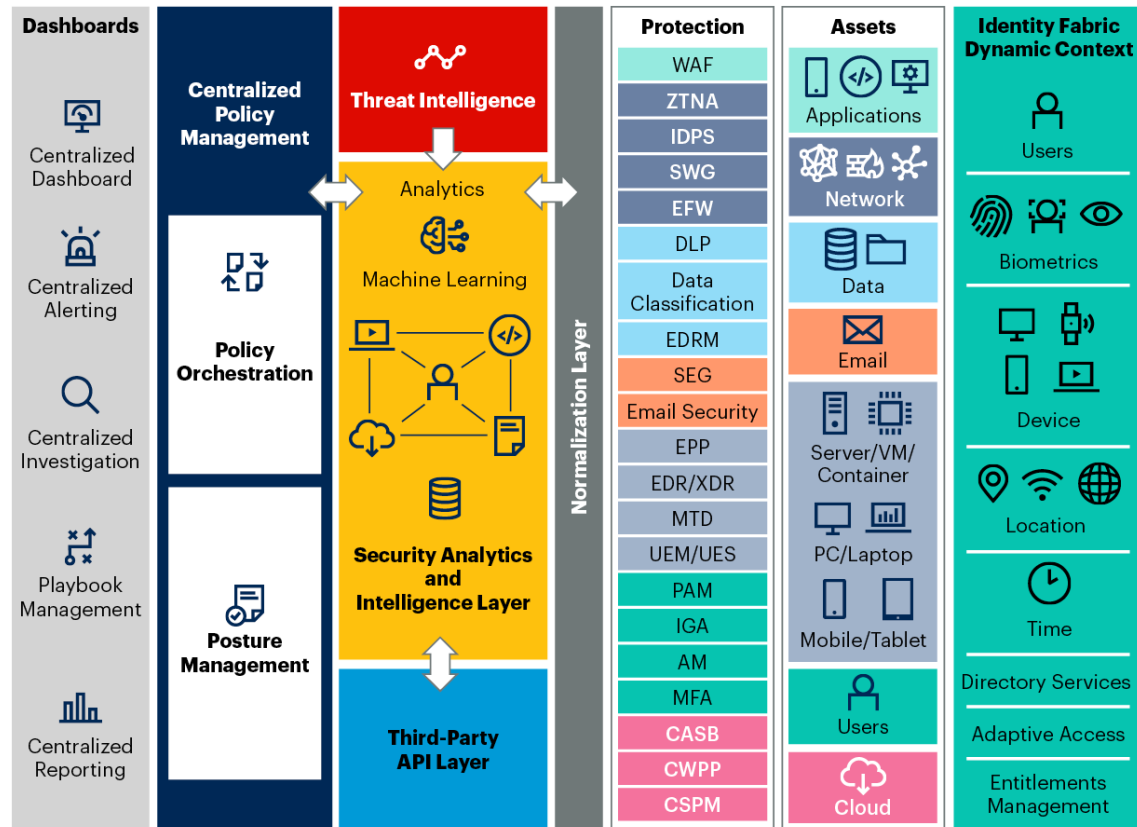
the context of the entire document. The Gartner document is available upon request from Fortinet.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

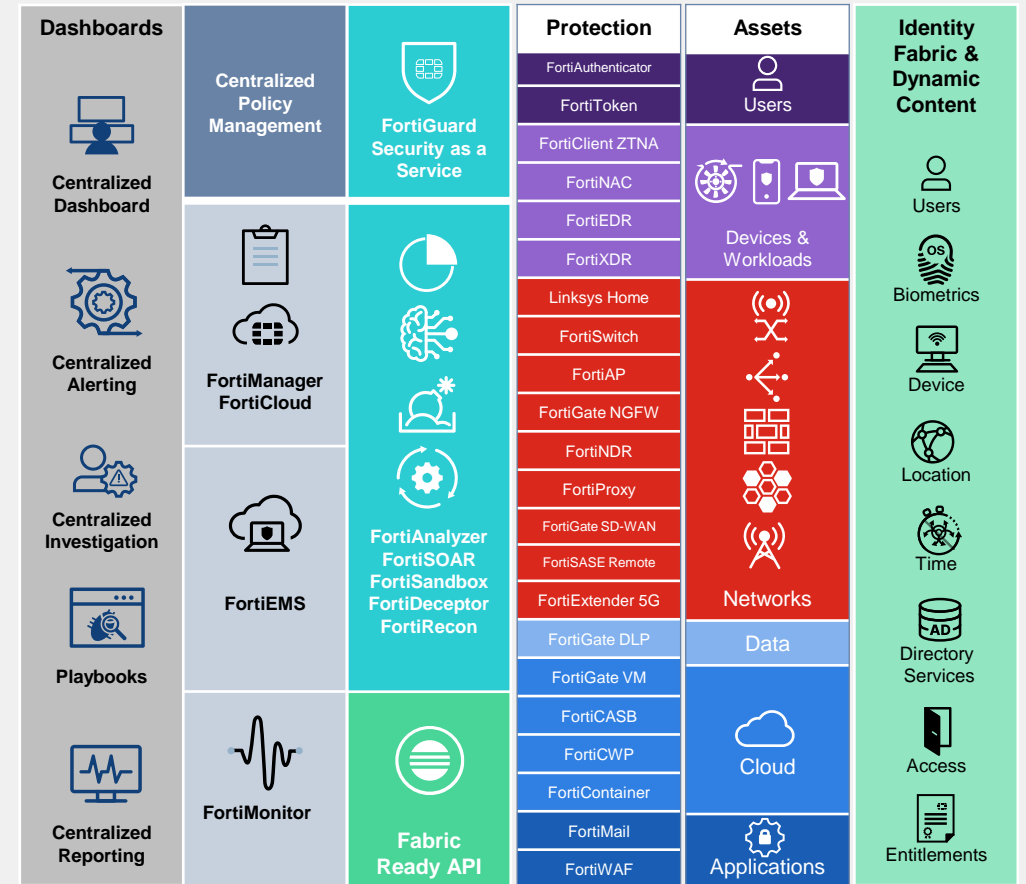
# Fortinet Makes Cybersecurity Mesh Architecture Possible



## Cybersecurity Mesh Architecture



Source: Gartner  
756156\_C



This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Fortinet.



GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

© Fortinet Inc. All Rights Reserved.

# Fortinet Broad Product Portfolio



## FortiGuard Security Services

### SOC & NOC

- Content Security
- Web Security
- Advanced SOC/NOC

### User Security

- User Security
- Device Security
- Bundled Security



## Fabric Management Center - SOC

### Endpoint

- FortiEDR
- FortiXDR

### Breach

- FortiSandbox
- FortiDeceptor
- FortiAI

### Incident Response

- FortiAnalyzer
- FortiSIEM
- FortiSOAR
- FortiGuard MDR Service



## Fabric Management Center - NOC

- FortiManager
- FortiCloud
- FortiMonitor



## Open Ecosystem

- Connector
- Fabric API
- DevOps
- Extended Fabric Ecosystem



## Zero Trust Access

- FortiClient
- FortiNAC
- FortiVoice
- FortiToken
- FortiAuthenticator
- FortiCamera



## Security-Driven Networking

### LAN Edge

- FortiAP
- FortiSwitch

### WAN Edge

- FortiGate SD-WAN
- FortiExtender

### DC Edge

- FortiGate
- FortiProxy

### Cloud Edge

- FortiSASE
- FortiSolator



## Adaptive Cloud Security

### Network

- FortiGate VM
- Multi-cloud SD-WAN
- FortiDDos

### Platform

- FortiCASB
- FortiCWP
- Cloud Security Posture Management

### Applications

- FortiWeb
- FortiMail
- FortiADC
- FortiGSMB



Appliance



VM



Hosted



Cloud



Software

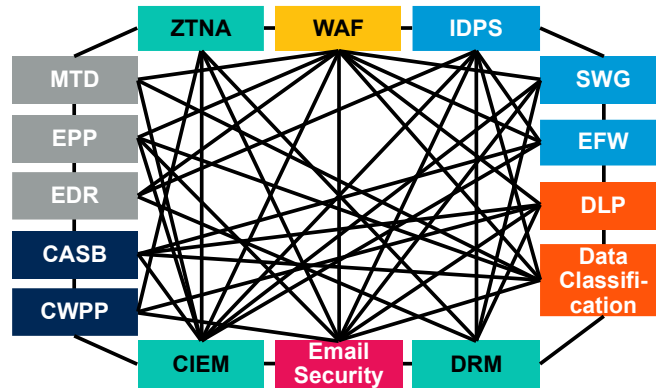


Container



# Key Takeaways

Gartner®



FORTINET®



**“By 2024, organizations adopting a cybersecurity mesh architecture to integrate security tools to work as a collaborative ecosystem will reduce the financial impact of individual security incidents by an average of 90%”**

*“Top Strategic Technology Trends for 2022: Cybersecurity Mesh, Felix Gaehtgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, Patrick Hevesi, 18 October 2021”*

*Executive Guide to Cybersecurity Mesh, 2022  
Felix Gaehtgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, Patrick Hevesi. As of October 2021*

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Fortinet.



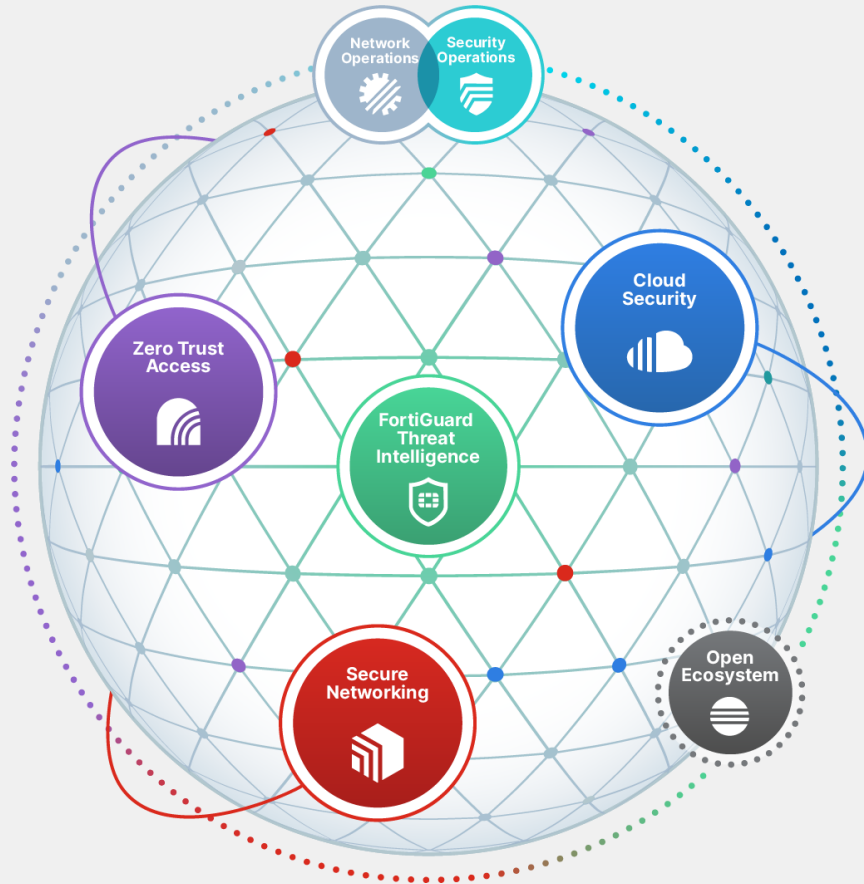
GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

© Fortinet Inc. All Rights Reserved.

**Fortinet Security Fabric delivers benefits of a cybersecurity mesh architecture today**

- Deep visibility across all edges
- Centrally managing distributed solutions
- Consistent enforcement of policies
- Real-time global threat intelligence across Fortinet Security Fabric deployments
- Automating actionable responses
- Broadest, most integrated open ecosystem

# If you remember nothing else...



**Fortinet Security Fabric is the cybersecurity mesh platform that delivers Gartner's cybersecurity mesh architecture**

## TODAY





**FORTINET®**

# Fortinet Customer Case Study

## Challenge

Large European Bank was having difficulty coping with:

- Expanding attack surface: cloud, campus, branch
- Partial visibility across the attack surface
- Inefficient security infrastructure contributing to high OPEX and capital expenses

## Solution Benefits

- Unified policy management and orchestration
- Coordinated security across all enforcement points
- Integrated visibility, fast detection and automated response
- Reduced complexity and increased Operational efficiency
- Readily benefit from FortiGuard Labs real-time intelligence and protection across all Fortinet Security Fabric deployments

