The use of OpenSSL in Common Criteria and FIPS 140 certifications

Martin Ukrop, *Red Hat, mukrop@redhat.com*
Vladimír Peňáz, *Masaryk University, vladi.penaz@gmail.com*

Red Hat

MASARYK UNIVERSITY

OpenAlt konference

Talk overview

1. What problem are we looking at?
   - Using OpenSSL as a use case
2. Preliminaries
   - Security certifications 101, sec-certs tool overview
3. Insights from Common Criteria
4. Insights from FIPS 140
5. Conclusions
   - Limitations, extensions, actionable steps

Part 1: What problem are we looking at?

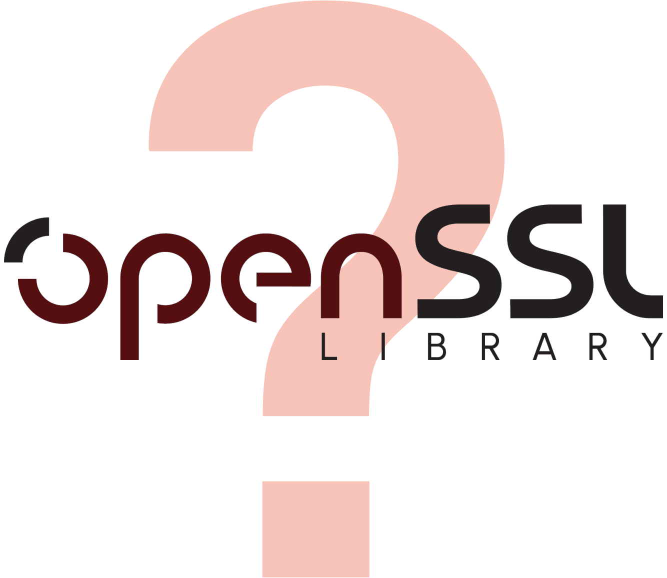
Who doesn’t love FOSS…?

(FOSS = Free and Open Source Software)

openSSL
LIBRARY

“We believe everyone should have access to security and privacy tools, whoever they are, wherever they are or whatever their personal beliefs are, as a fundamental human right.”

Deficiencies of FOSS



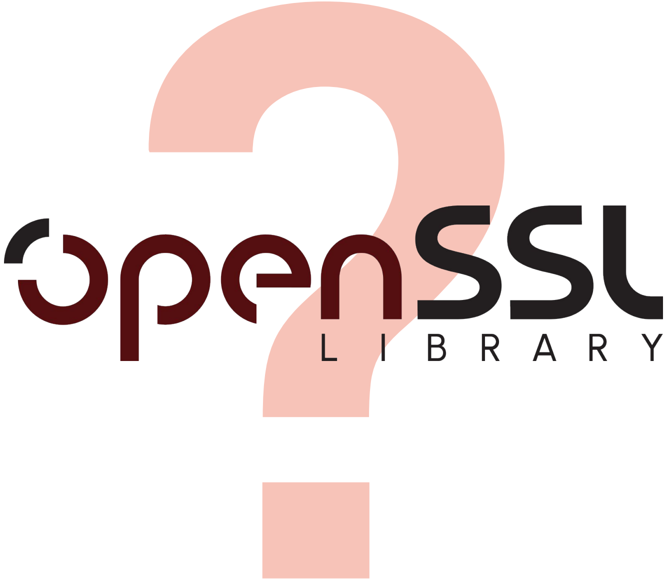
Deficiencies of FOSS

- How prevalent is it?
    - Prestige, negotiation position for funding

openSSL
LIBRARY

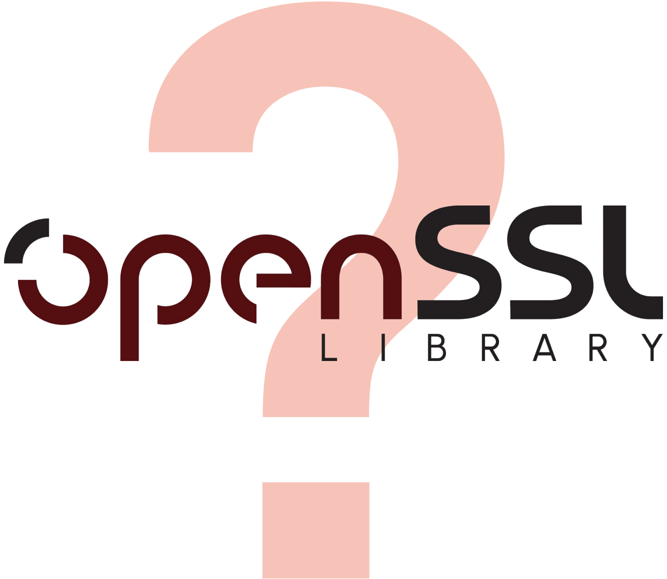
Deficiencies of FOSS

- How prevalent is it?
  - Prestige, negotiation position for funding
- Which versions are commonly used?
  - User behavior, security implications



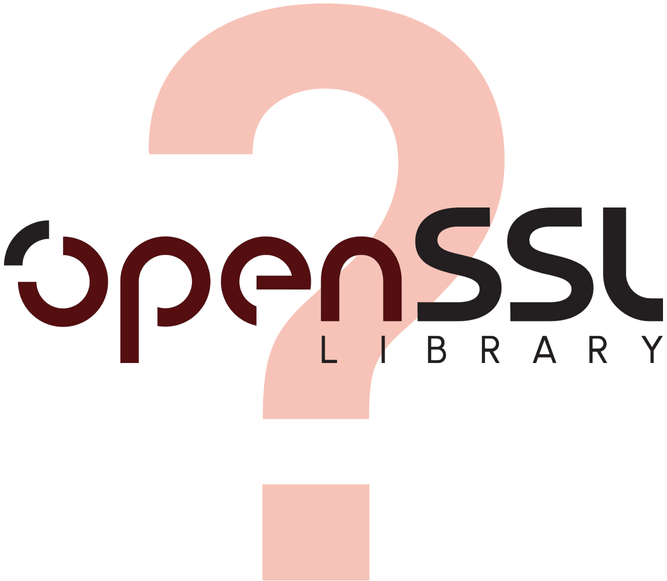
Deficiencies of FOSS

- How prevalent is it?
    - Prestige, negotiation position for funding
- Which versions are commonly used?
    - User behavior, security implications
- Which vendors use it?
    - Potential for cooperation or business



Deficiencies of FOSS

- How prevalent is it?
  - Prestige, negotiation position for funding
- Which versions are commonly used?
  - User behavior, security implications
- Which vendors use it?
  - Potential for cooperation or business
- What products use it?
  - Feature prioritization, roadmap adjustments



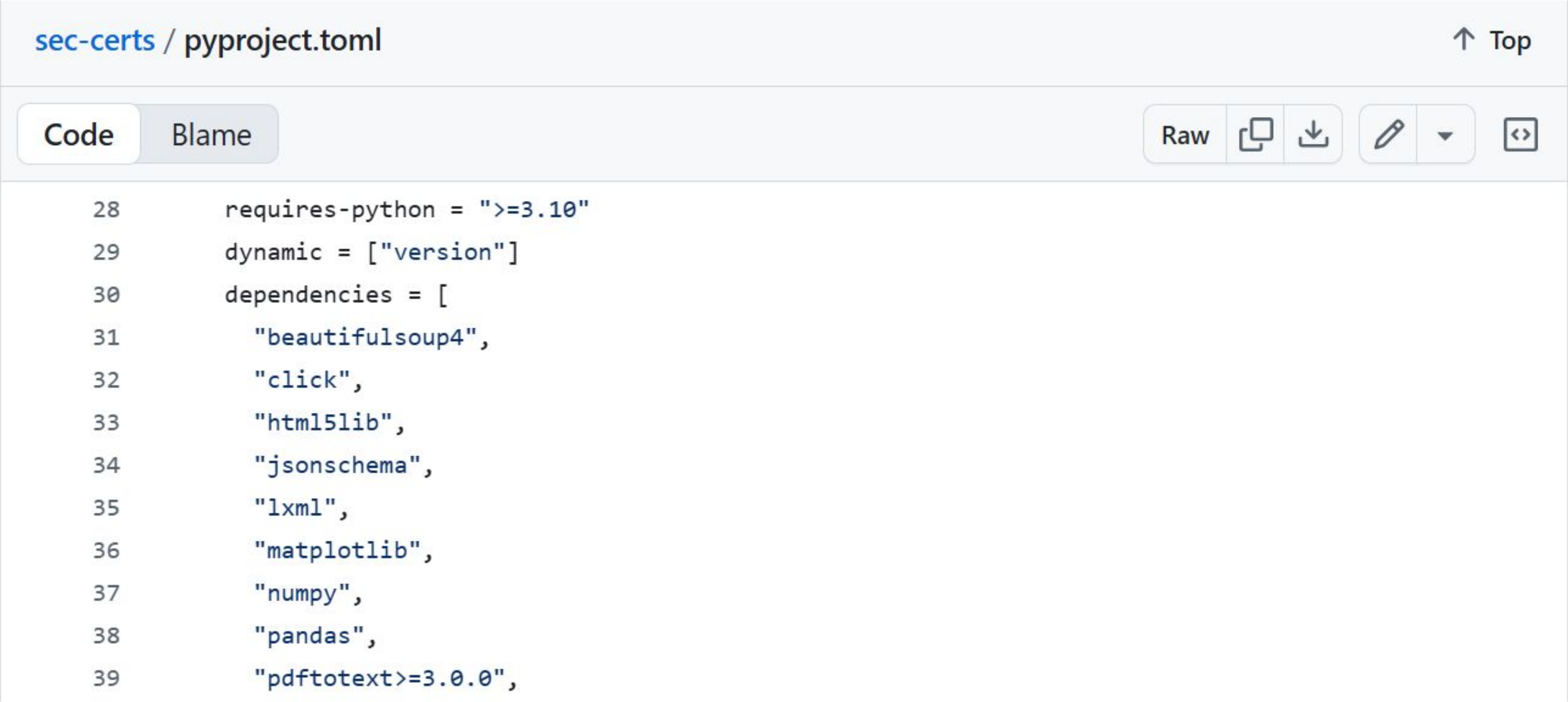
Deficiencies of FOSS

- How prevalent is it?
    - Prestige, negotiation position for funding
- Which versions are commonly used?
    - User behavior, security implications
- Which vendors use it?
    - Potential for cooperation or business
- What products use it?
    - Feature prioritization, roadmap adjustments
- What alternatives are used?
    - Insights into the dynamics of forks and competition

openSSL
LIBRARY

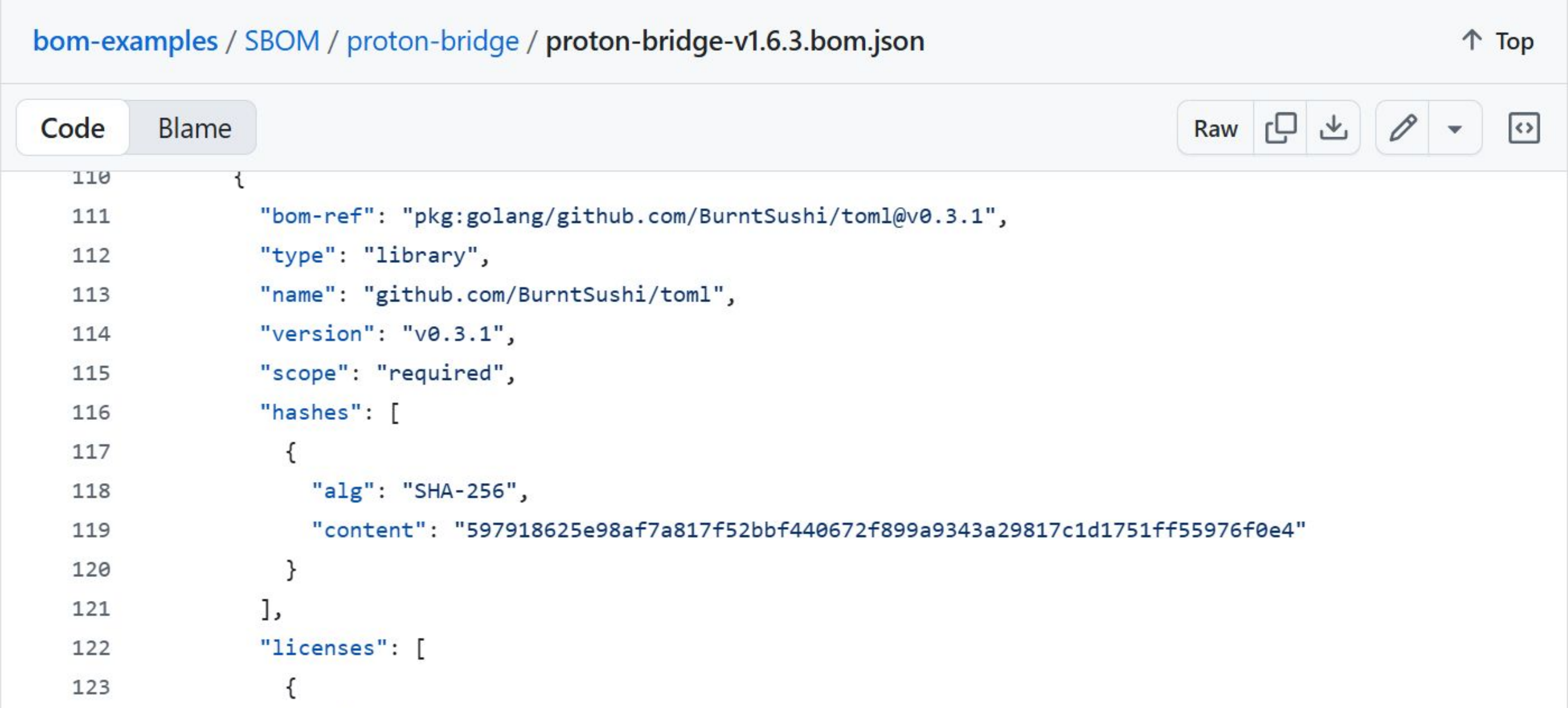
Proxy 1: Product component information

Proxy 1a: FOSS with transparent sources



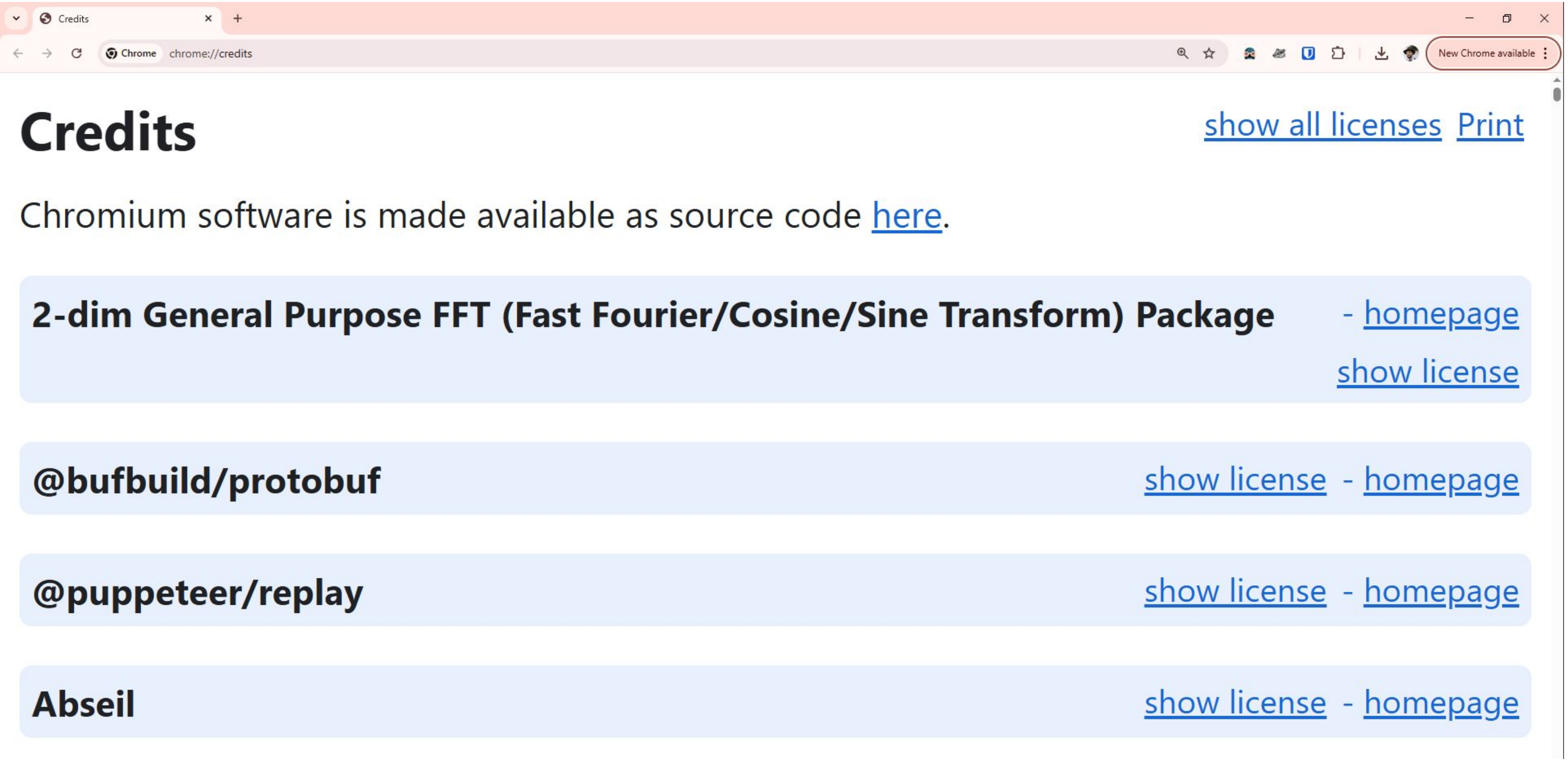
```
requires-python = ">=3.10"
dynamic = ["version"]
dependencies = [
  "beautifulsoup4",
  "click",
  "html5lib",
  "jsonschema",
  "lxml",
  "matplotlib",
  "numpy",
  "pandas",
  "pdftotext>=3.0.0",
```

Proxy 1b: Software Bill of Materials (SBOMs)


bom-examples / SBOM / proton-bridge / proton-bridge-v1.6.3.bom.json
Top
Code
Blame
Raw

```
        {
          "bom-ref": "pkg:golang/github.com/BurntSushi/toml@v0.3.1",
          "type": "library",
          "name": "github.com/BurntSushi/toml",
          "version": "v0.3.1",
          "scope": "required",
          "hashes": [
            {
              "alg": "SHA-256",
              "content": "597918625e98af7a817f52bbf440672f899a9343a29817c1d1751ff55976f0e4"
            }
          ],
          "licenses": [
            {
```

Proxy 1c: Legal licence notices



Credits

show all licenses Print

Chromium software is made available as source code here.

2-dim General Purpose FFT (Fast Fourier/Cosine/Sine Transform) Package - homepage show license

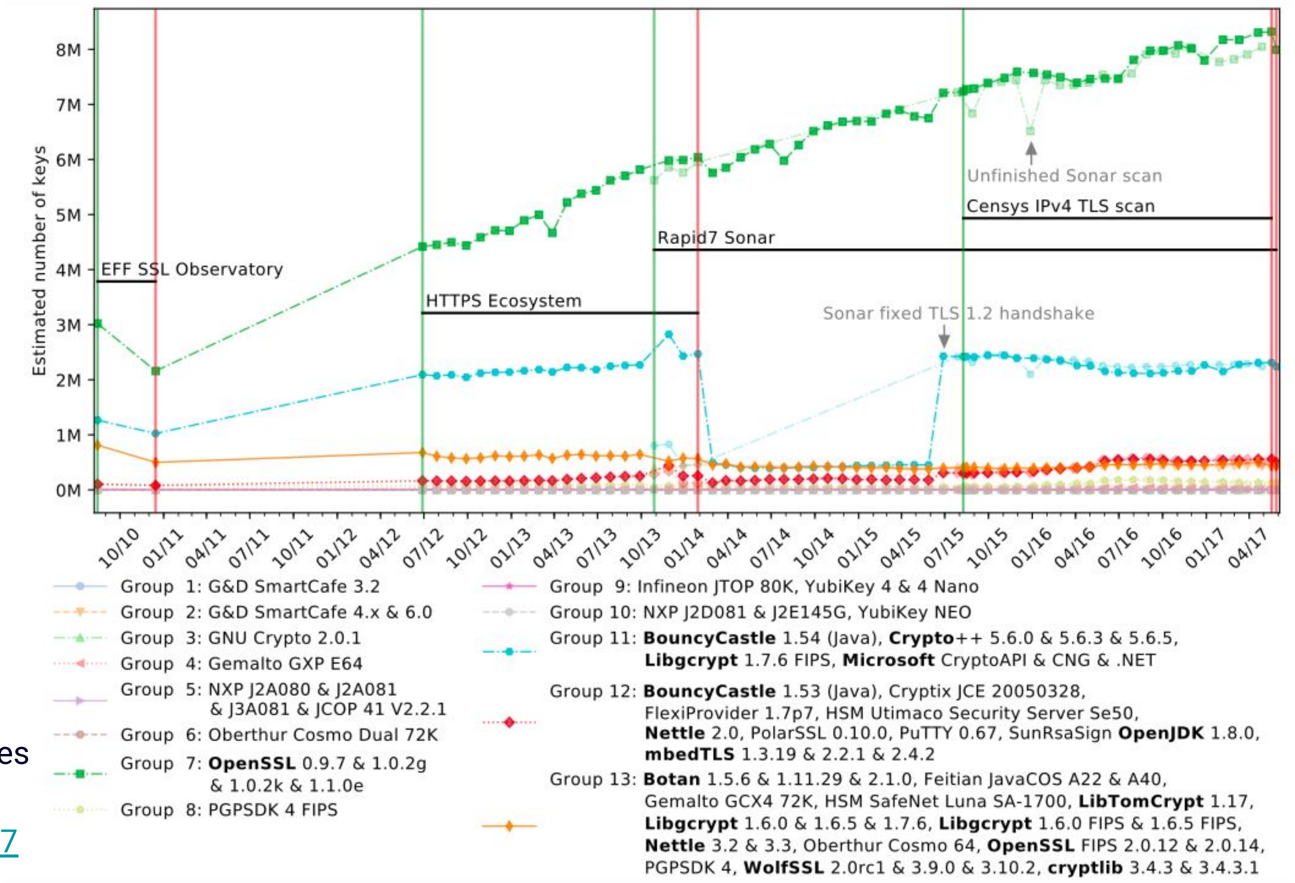
@bufbuild/protobuf show license - homepage

@puppeteer/replay show license - homepage

Abseil show license - homepage

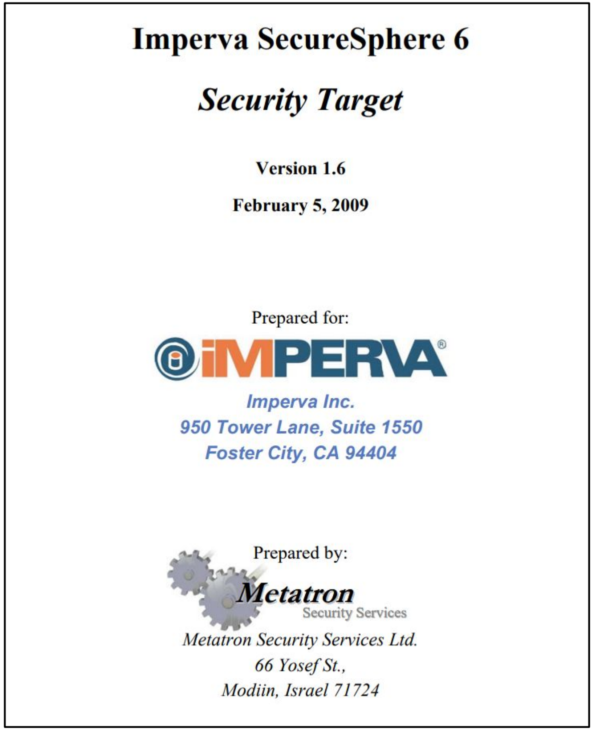
Proxy 2: Public data artefacts

(e.g. Internet scans)



ACSAC 2017: Measuring Popularity of Cryptographic Libraries in Internet-Wide Scans
crocs.fi.muni.cz/papers/acsac2017

Proxy 3: Certification documents



Imperva SecureSphere 6

Security Target

Version 1.6

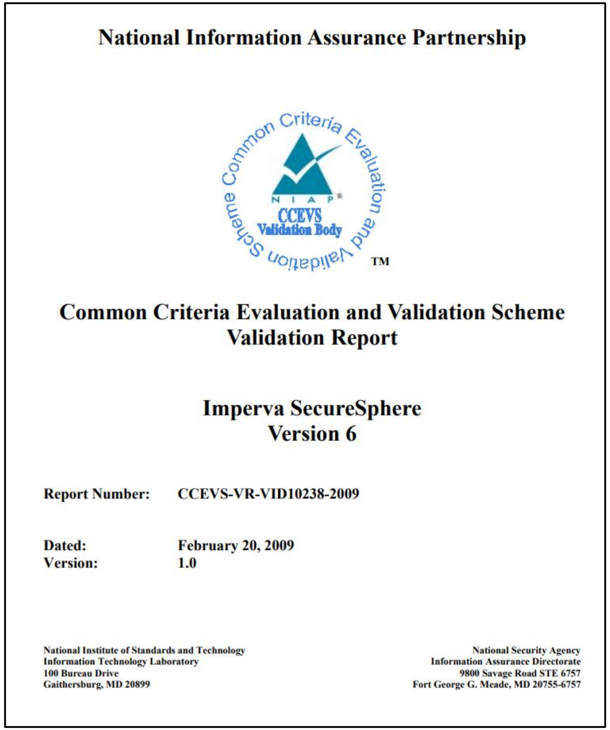
February 5, 2009

Prepared for:

Imperva Inc.
950 Tower Lane, Suite 1550
Foster City, CA 94404

Prepared by:

Metatron Security Services Ltd.
66 Yosef St.,
Modiin, Israel 71724



National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Imperva SecureSphere
Version 6

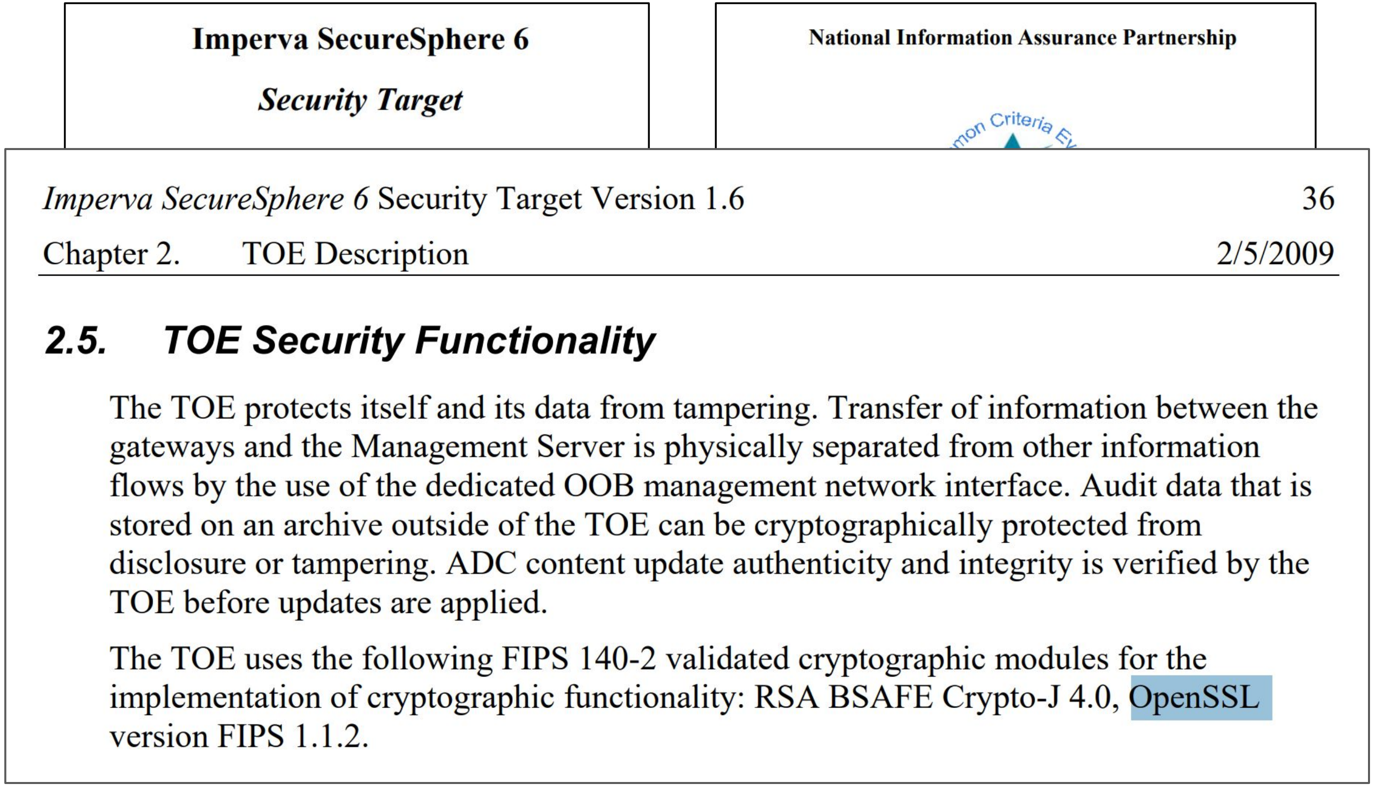
Report Number: CCEVS-VR-VID10238-2009

Dated: February 20, 2009
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6757
Fort George G. Meade, MD 20755-6757

Proxy 3: Certification documents



Imperva SecureSphere 6

Security Target

National Information Assurance Partnership

mon Criteria Ev

Imperva SecureSphere 6 Security Target Version 1.6 36

Chapter 2. TOE Description 2/5/2009

2.5. TOE Security Functionality

The TOE protects itself and its data from tampering. Transfer of information between the gateways and the Management Server is physically separated from other information flows by the use of the dedicated OOB management network interface. Audit data that is stored on an archive outside of the TOE can be cryptographically protected from disclosure or tampering. ADC content update authenticity and integrity is verified by the TOE before updates are applied.

The TOE uses the following FIPS 140-2 validated cryptographic modules for the implementation of cryptographic functionality: RSA BSAFE Crypto-J 4.0, OpenSSL version FIPS 1.1.2.

The big picture

- FOSS: Open means little awareness/control of use
    - *However: Estimations from proxies and side-channels*
- Proxy 1: Product component information
    - FOSS with transparent sources, Software Bill of Materials (SBOMs), Legal licence notices
    - *However: FOSS only, still not standard, lack of automation*
- Proxy 2: Public data artefacts
    - E.g. Internet scans
    - *However: Only products with public artifacts*
- Proxy 3: Certification documents
    - Common Criteria, FIPS 140, EUCC, FedRAMP, SOC, ...
    - *However: not harmonized, lack of automation*

The big picture

- FOSS: Open means little awareness/control of use
  - *However: Estimations from proxies and side-channels*
- Proxy 1: Product component information
  - FOSS with transparent sources, Software Bill of Materials (SBOMs), Legal licence notices
  - *However: FOSS only, still not standard, lack of automation*
- Proxy 2: Public data artefacts
  - E.g. Internet scans
  - *However: Only products with public artifacts*
- Proxy 3: Certification documents
  - Common Criteria, FIPS 140, EUCC, FedRAMP, SOC …
  - *However: not harmonized, lack of automation*

How much data can we mine here? (about OpenSSL)

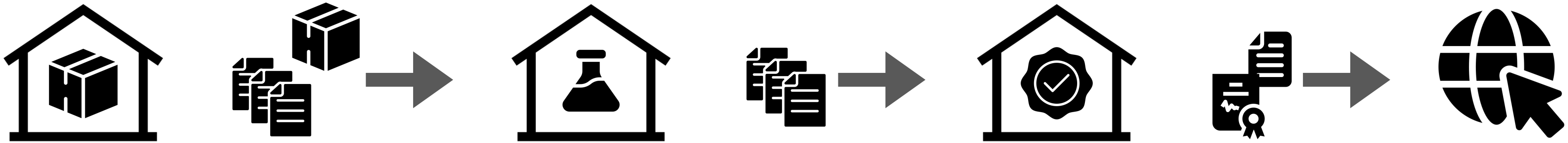
Part 2: Preliminaries

Security certifications 101 (simplified and incorrect 🙂)

- **Idea: Increase security by independent audits**
- Many schemes exist: Common Criteria, FIPS 140, FedRAMP, ISO 27k, SOC, …

Security certifications 101 (simplified and incorrect 🙂)

- **Idea: Increase security by independent audits**
- Many schemes exist: Common Criteria, FIPS 140, FedRAMP, ISO 27k, SOC, …



vendor

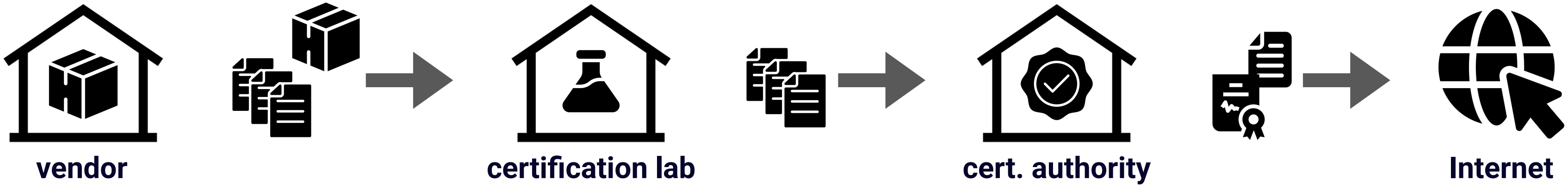
certification lab

cert. authority

Internet

Security certifications 101 (simplified and incorrect 🙂)

- **Idea: Increase security by independent audits**
- Many schemes exist: Common Criteria, FIPS 140, FedRAMP, ISO 27k, SOC, …



vendor → certification lab → cert. authority → Internet

Common Criteria for Information Technology Security Evaluation

- For **products**
- International (ISO standard)
- National schemes (“authorities”)

FIPS 140 (Federal Information Processing Standard)

- For **cryptographic modules**
- Originally USA+CA,
  today ISO standard (global)

The sec-certs tool

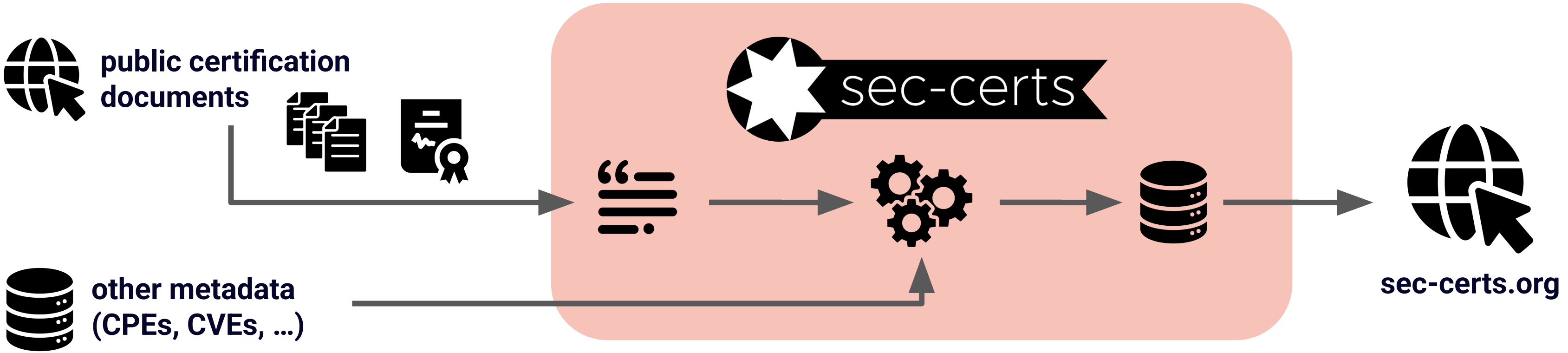
- **Idea: Allow ecosystem exploration within CC + FIPS 140**
- Open source + open data + public website

* This project is supported by the European Union under Grant Agreement No. 101087529 (CHESS).

The sec-certs tool

sec-certs

- **Idea: Allow ecosystem exploration within CC + FIPS 140**
- Open source + open data + public website



public certification documents

other metadata (CPEs, CVEs, …)

sec-certs

sec-certs.org

MASARYK UNIVERSITY

CROCS
Centre for Research on Cryptography and Security

Red Hat

CHESS

Co-funded by the European Union

* This project is supported by the European Union under Grant Agreement No. 101087529 (CHESS).

Part 3: Insights from Common Criteria

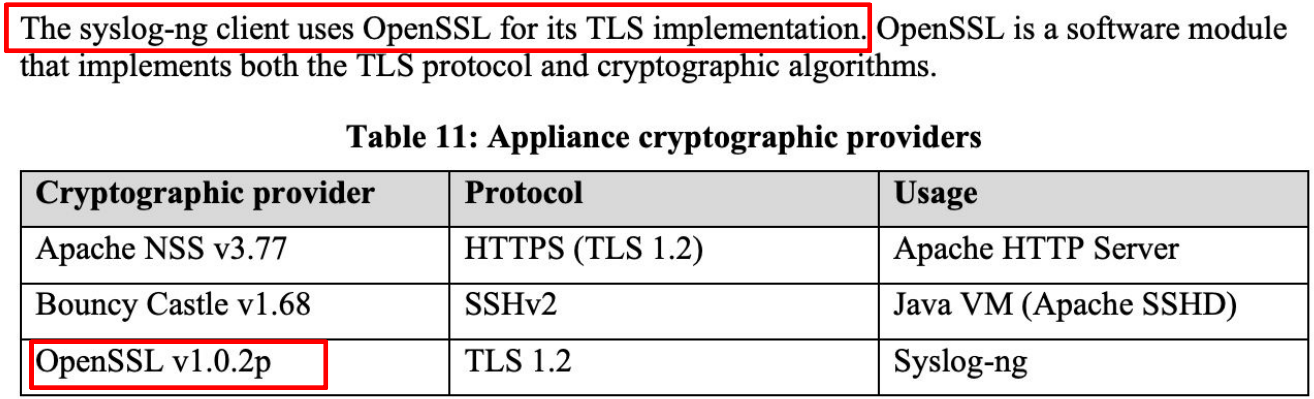
How prevalent is OpenSSL in certified products?

How prevalent is OpenSSL in certified products?

- **OpenSSL is mentioned 7 555 times** in public CC certification files
    - For comparison: There are 6 446 CC certificates

How prevalent is OpenSSL in certified products?

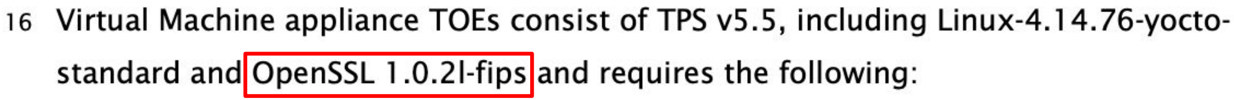
- **OpenSSL is mentioned 7 555 times** in public CC certification files
  - For comparison: There are 6 446 CC certificates



The syslog-ng client uses OpenSSL for its TLS implementation. OpenSSL is a software module that implements both the TLS protocol and cryptographic algorithms.

Table 11: Appliance cryptographic providers

Cryptographic provider	Protocol	Usage
Apache NSS v3.77	HTTPS (TLS 1.2)	Apache HTTP Server
Bouncy Castle v1.68	SSHv2	Java VM (Apache SSHD)
OpenSSL v1.0.2p	TLS 1.2	Syslog-ng

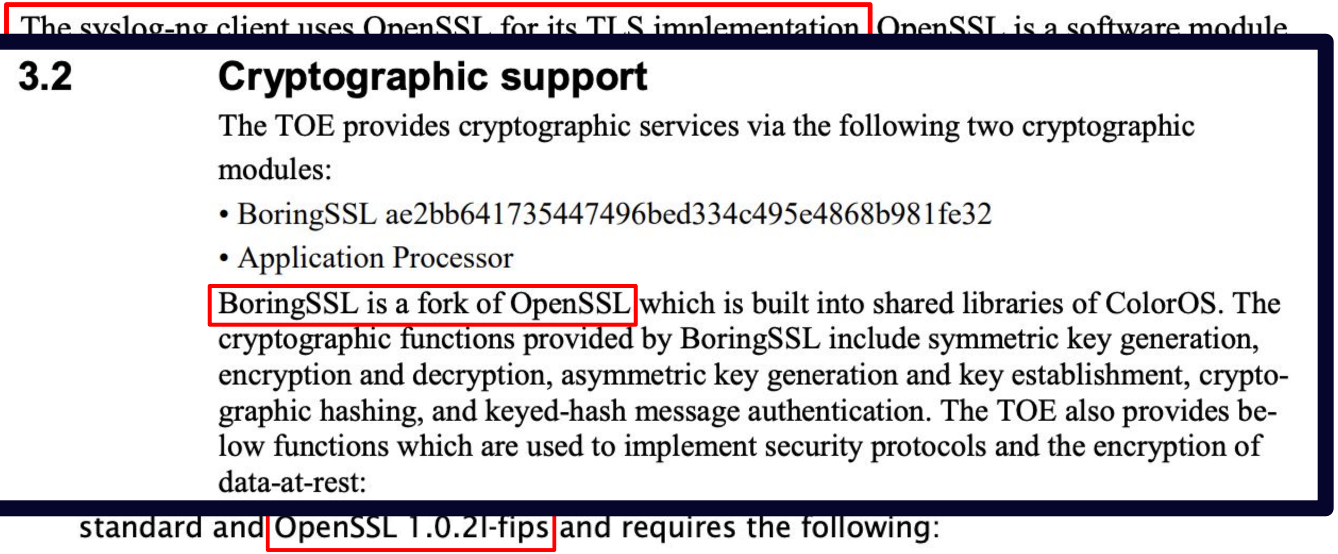


16 Virtual Machine appliance TOEs consist of TPS v5.5, including Linux-4.14.76-yocto-standard and OpenSSL 1.0.2l-fips and requires the following:

Sources: CCEVS-VR-VID-11178-2023, ISCB-5-RPT-C128-CR-v1a

How prevalent is OpenSSL in certified products?

- **OpenSSL is mentioned 7 555 times** in public CC certification files
    - For comparison: There are 6 446 CC certificates



The syslog-ng client uses OpenSSL for its TLS implementation. OpenSSL is a software module

3.2 Cryptographic support

The TOE provides cryptographic services via the following two cryptographic modules:

- BoringSSL ae2bb641735447496bed334c495e4868b981fe32
- Application Processor

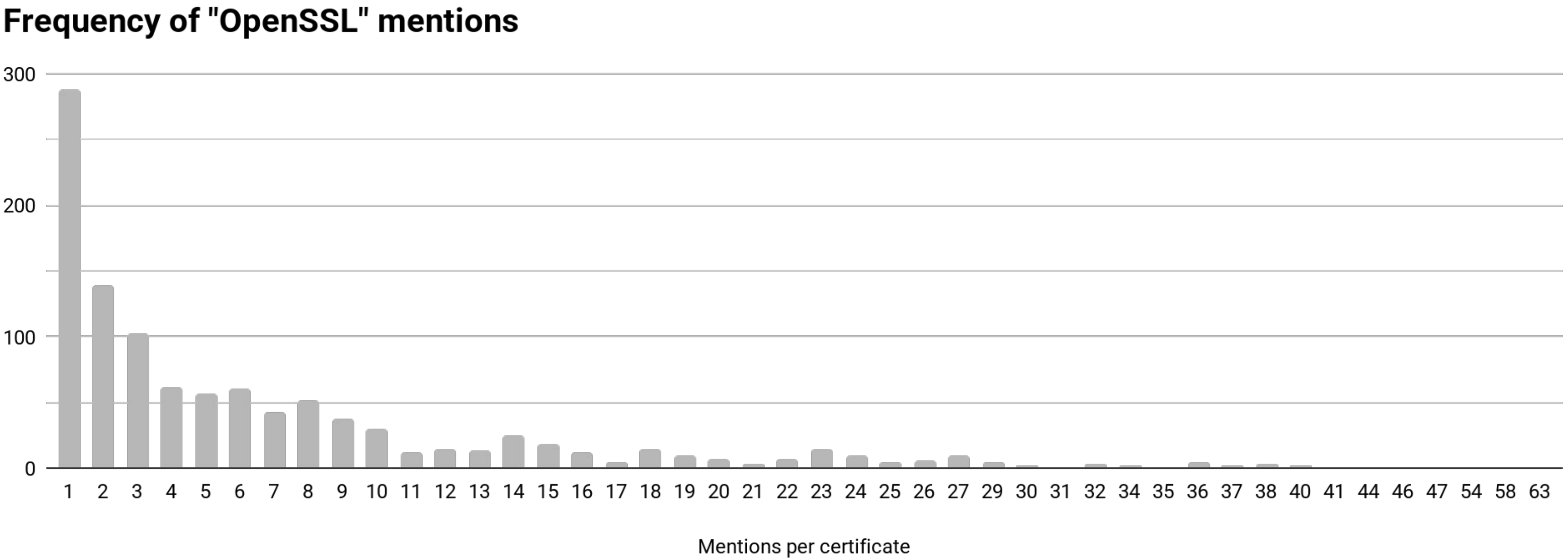
BoringSSL is a fork of OpenSSL which is built into shared libraries of ColorOS. The cryptographic functions provided by BoringSSL include symmetric key generation, encryption and decryption, asymmetric key generation and key establishment, cryptographic hashing, and keyed-hash message authentication. The TOE also provides below functions which are used to implement security protocols and the encryption of data-at-rest:

standard and OpenSSL 1.0.2l-fips and requires the following:

Sources: CCEVS-VR-VID-11178-2023, ISCB-5-RPT-C128-CR-v1a, CSEC2021007

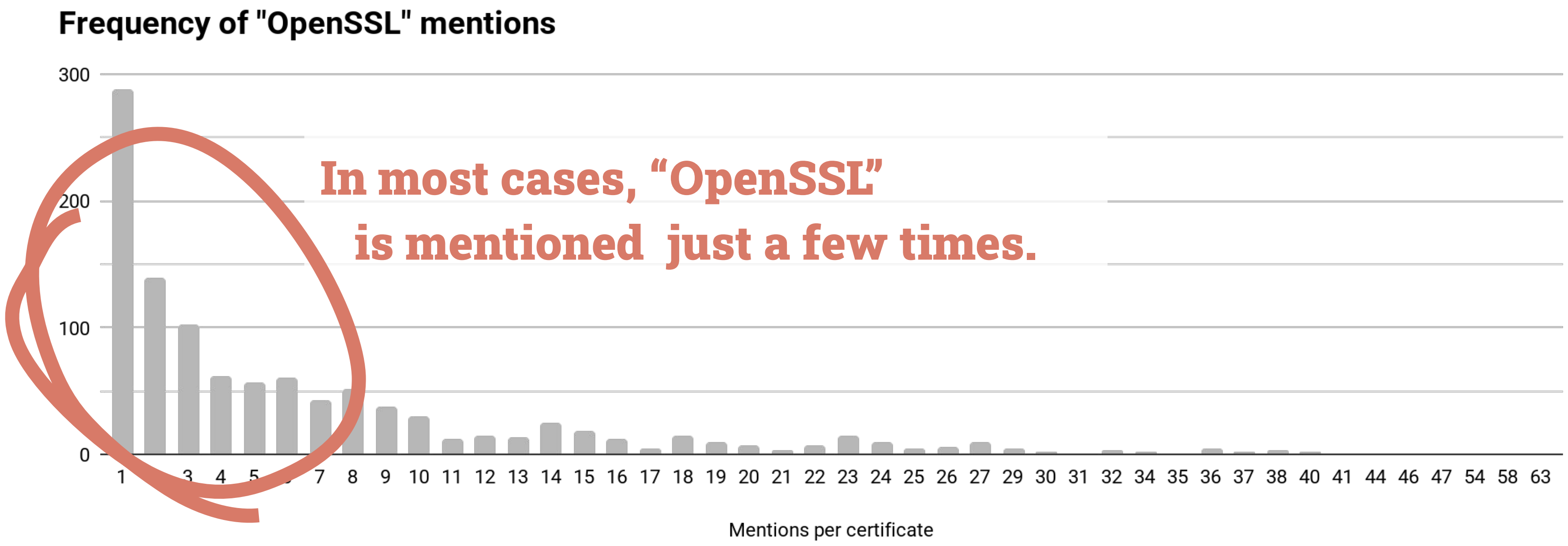
How prevalent is OpenSSL in certified products?

- **OpenSSL is mentioned 7 555 times** in public CC certification files
    - For comparison: There are 6 446 CC certificates



How prevalent is OpenSSL in certified products?

- **OpenSSL is mentioned 7 555 times** in public CC certification files
  - For comparison: There are 6 446 CC certificates



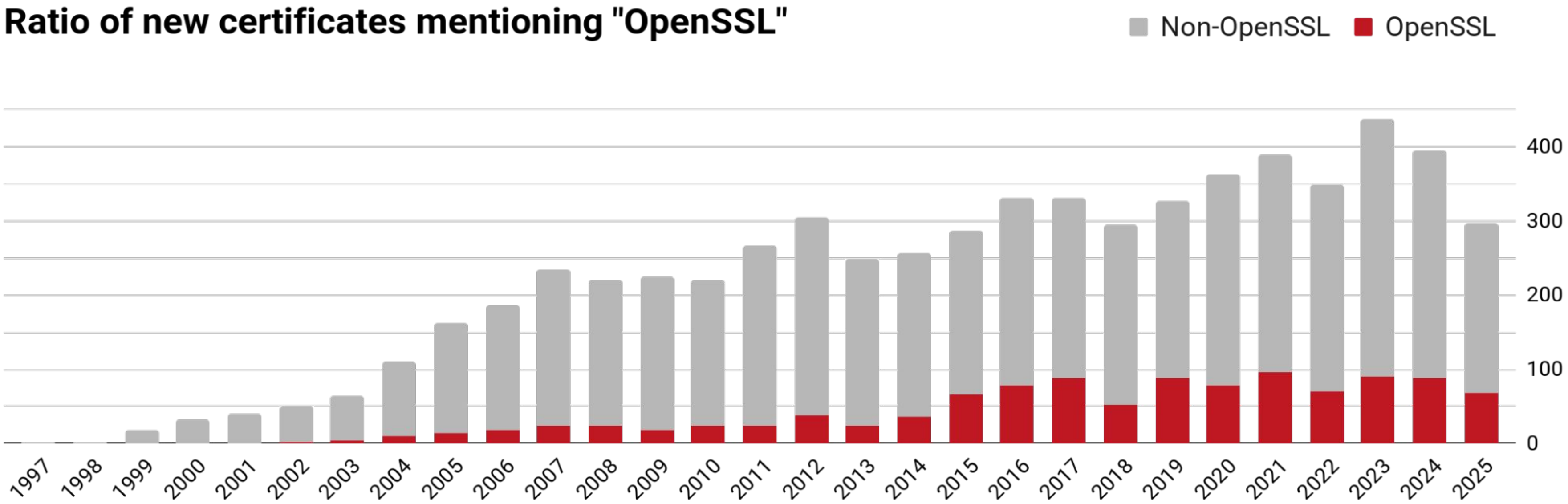
In most cases, "OpenSSL" is mentioned just a few times.

How prevalent is OpenSSL in certified products?

- **OpenSSL is mentioned in 1 084 distinct CC certificates (~17%)**
    - For comparison: There are 6 446 CC certificates

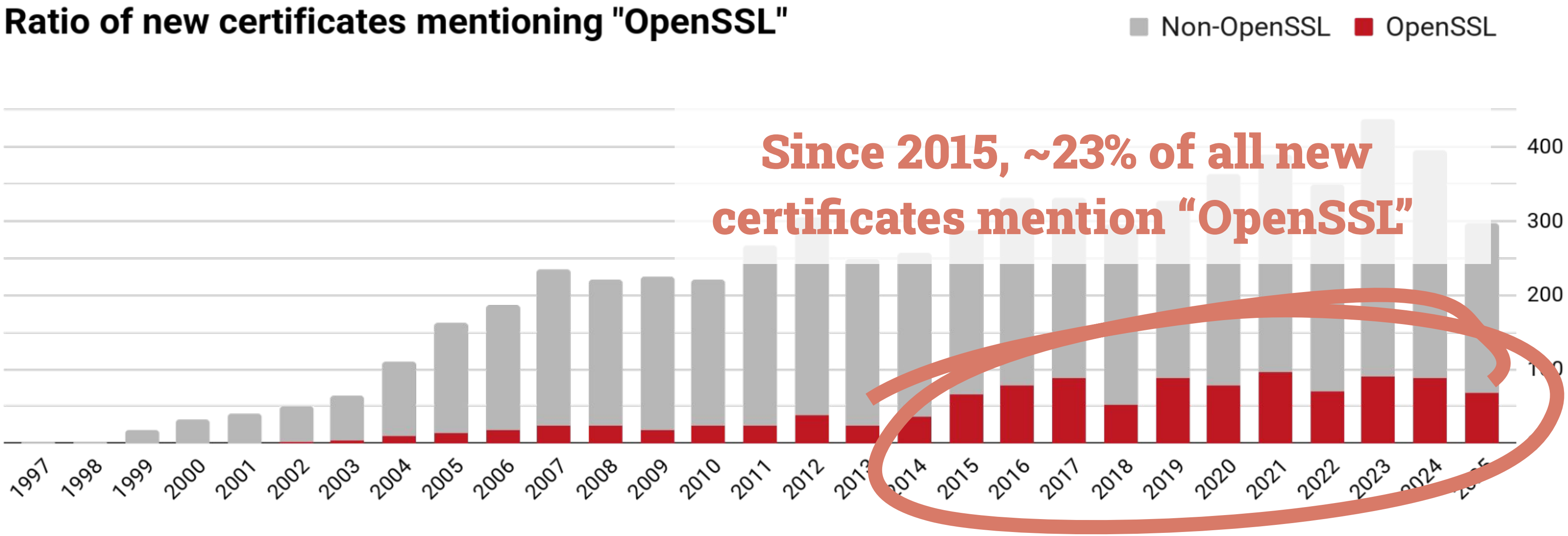
How prevalent is OpenSSL in certified products?

- **OpenSSL is mentioned in 1 084 distinct CC certificates (~17%)**
    - For comparison: There are 6 446 CC certificates



How prevalent is OpenSSL in certified products?

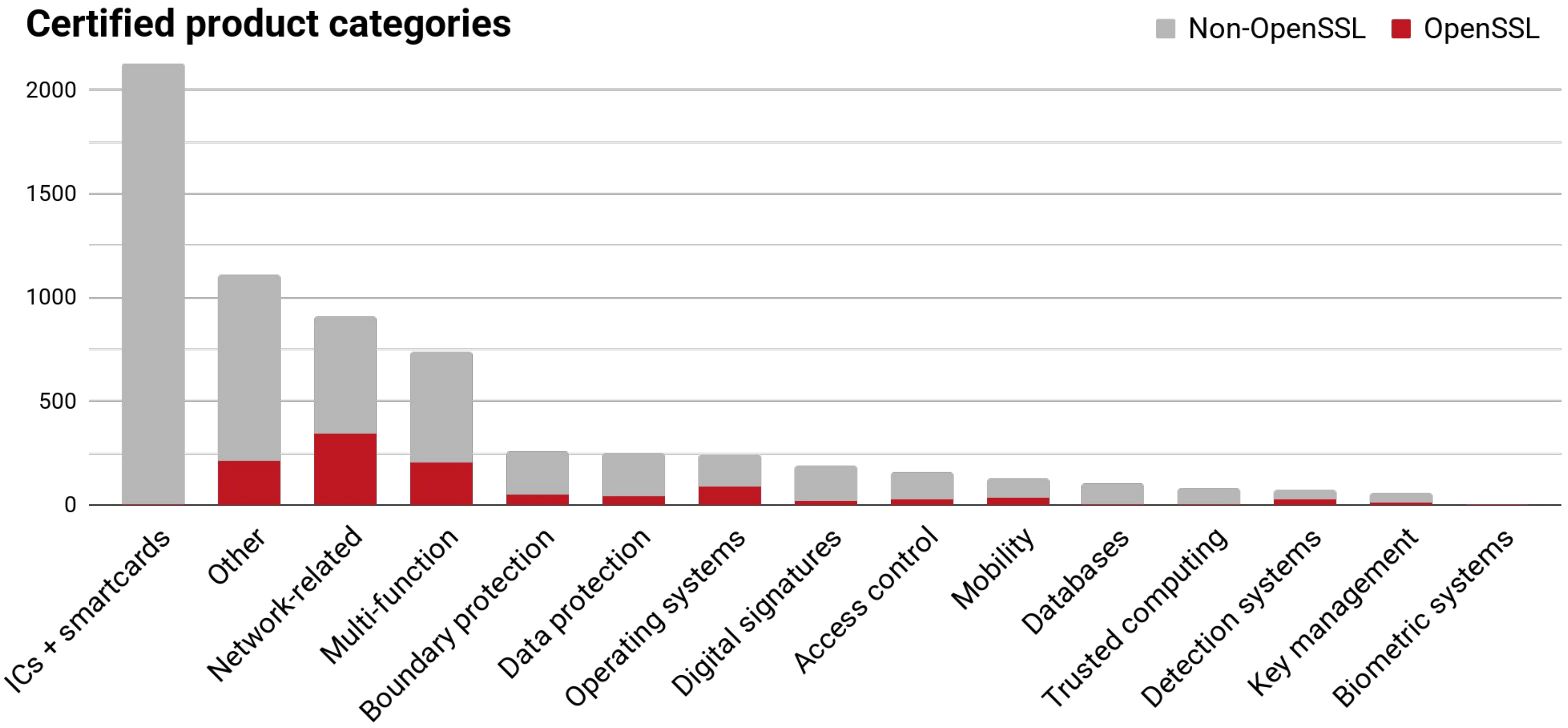
- **OpenSSL is mentioned in 1 084 distinct CC certificates (~17%)**
  - For comparison: There are 6 446 CC certificates



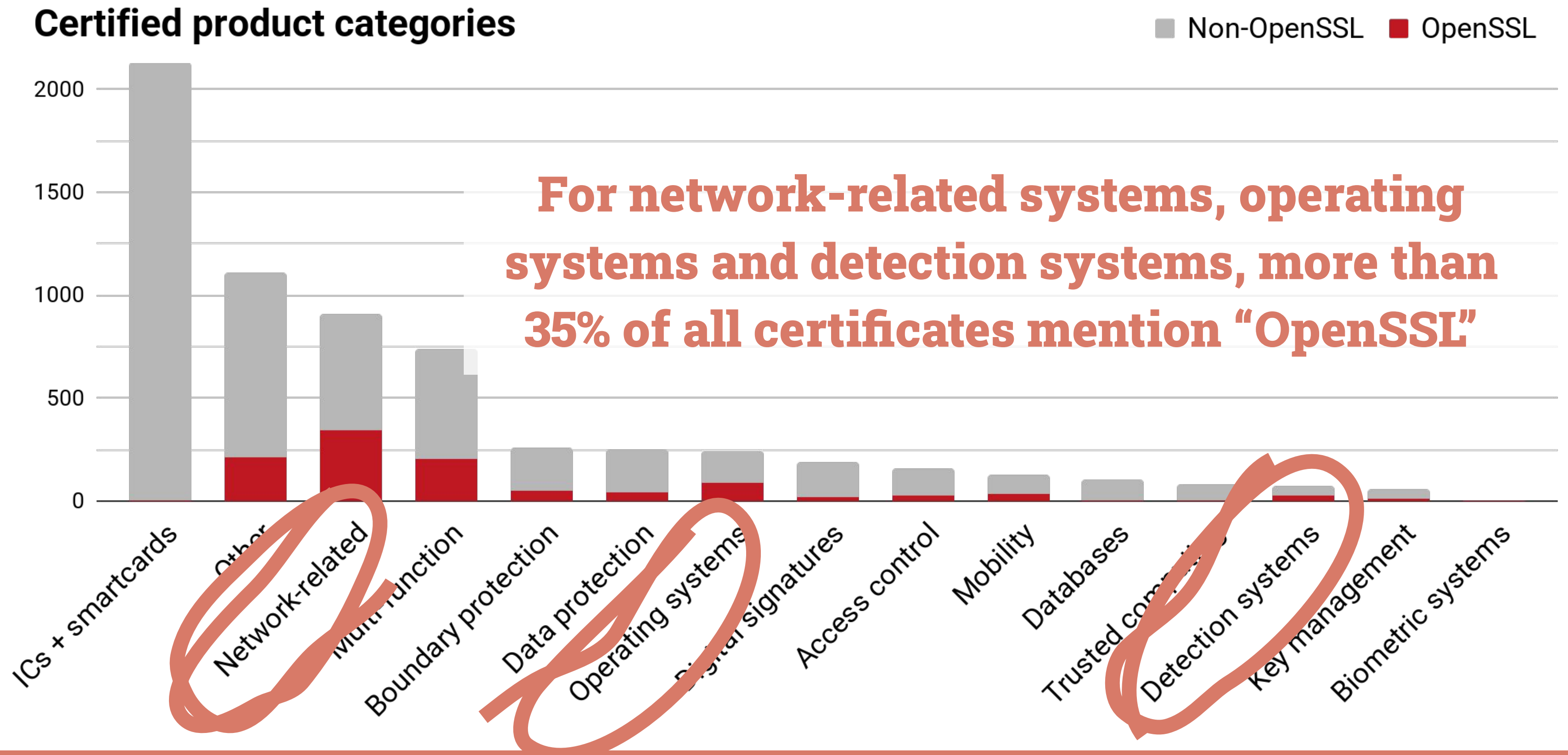
Since 2015, ~23% of all new certificates mention “OpenSSL”

What kind of certified products use OpenSSL?

What kind of certified products use OpenSSL?



What kind of certified products use OpenSSL?



For network-related systems, operating systems and detection systems, more than 35% of all certificates mention "OpenSSL"

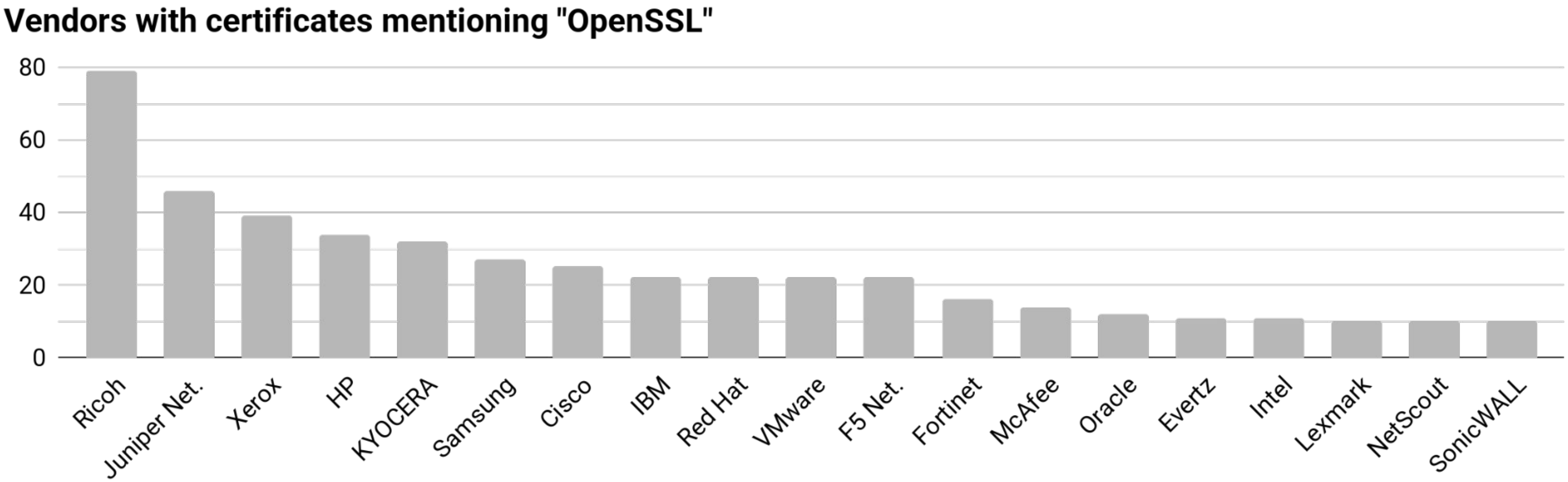
Who uses OpenSSL in their certified products?

Who uses OpenSSL in their certified products?

- **313 distinct vendors mention OpenSSL** is their CC certificates (~28%)
    - For comparison: There are 1 124 vendors in the CC dataset
    - Only 46 vendors (~15%) have 5+ certificates

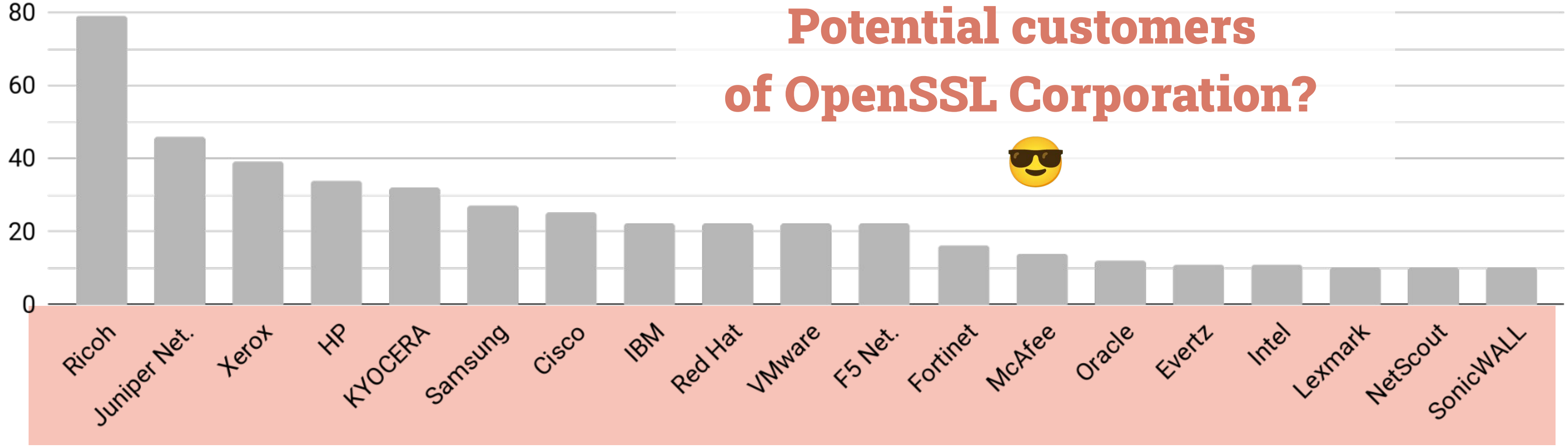
Who uses OpenSSL in their certified products?

- **313 distinct vendors mention OpenSSL** is their CC certificates (~28%)
  - For comparison: There are 1 124 vendors in the CC dataset
  - Only 46 vendors (~15%) have 5+ certificates



Who uses OpenSSL in their certified products?

- **313 distinct vendors mention OpenSSL** is their CC certificates (~28%)
    - For comparison: There are 1 124 vendors in the CC dataset
    - Only 46 vendors (~15%) have 5+ certificates

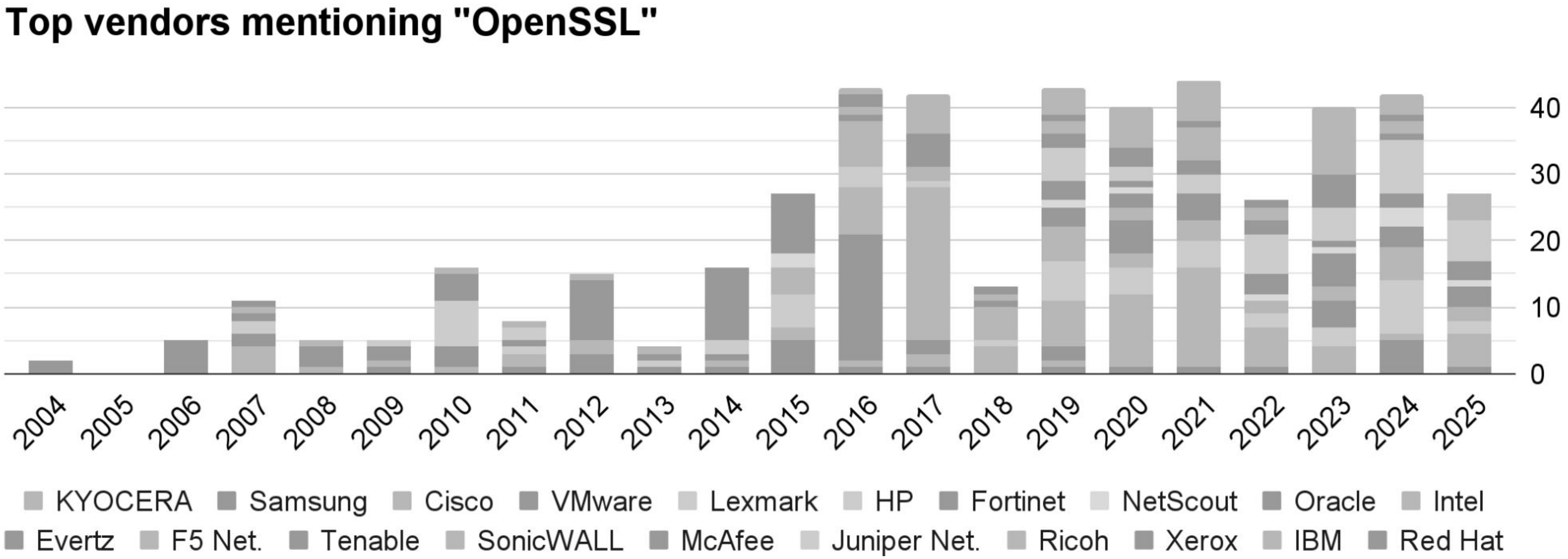


Vendors with certificates mentioning "OpenSSL"

Potential customers of OpenSSL Corporation? 😎

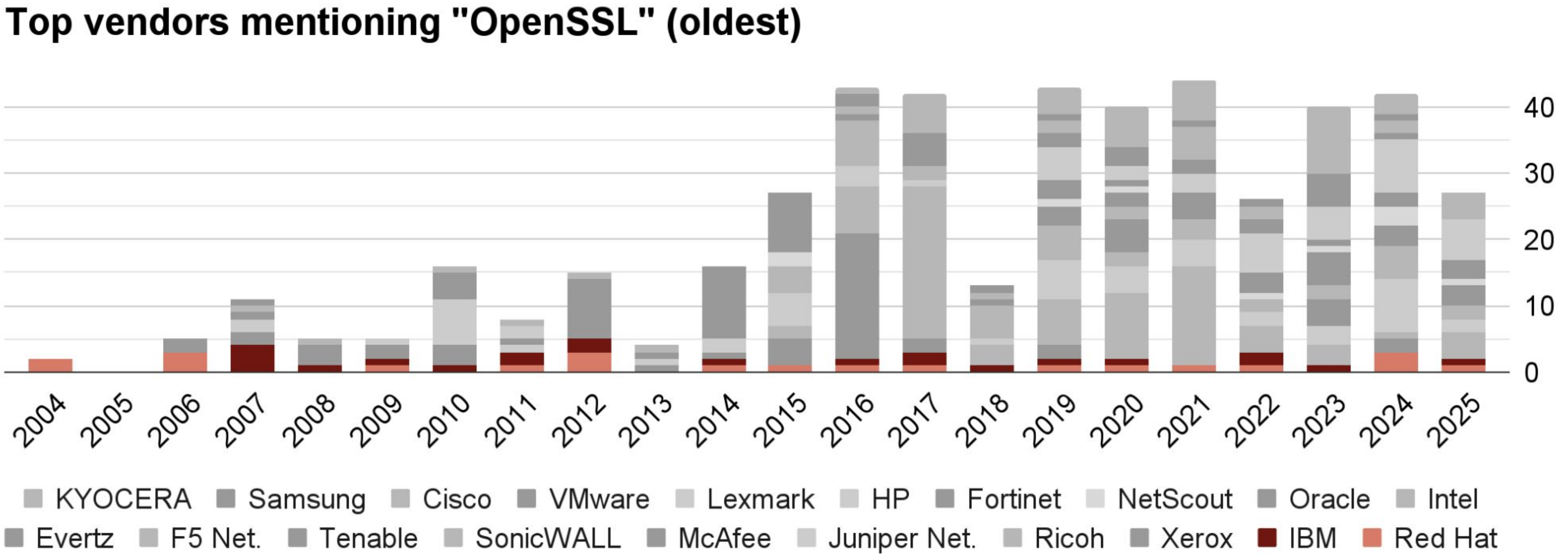
Who uses OpenSSL in their certified products?

- **313 distinct vendors mention OpenSSL** is their CC certificates (~28%)
    - For comparison: There are 1 124 vendors in the CC dataset
    - Only 46 vendors (~15%) have 5+ certificates


Top vendors mentioning "OpenSSL"

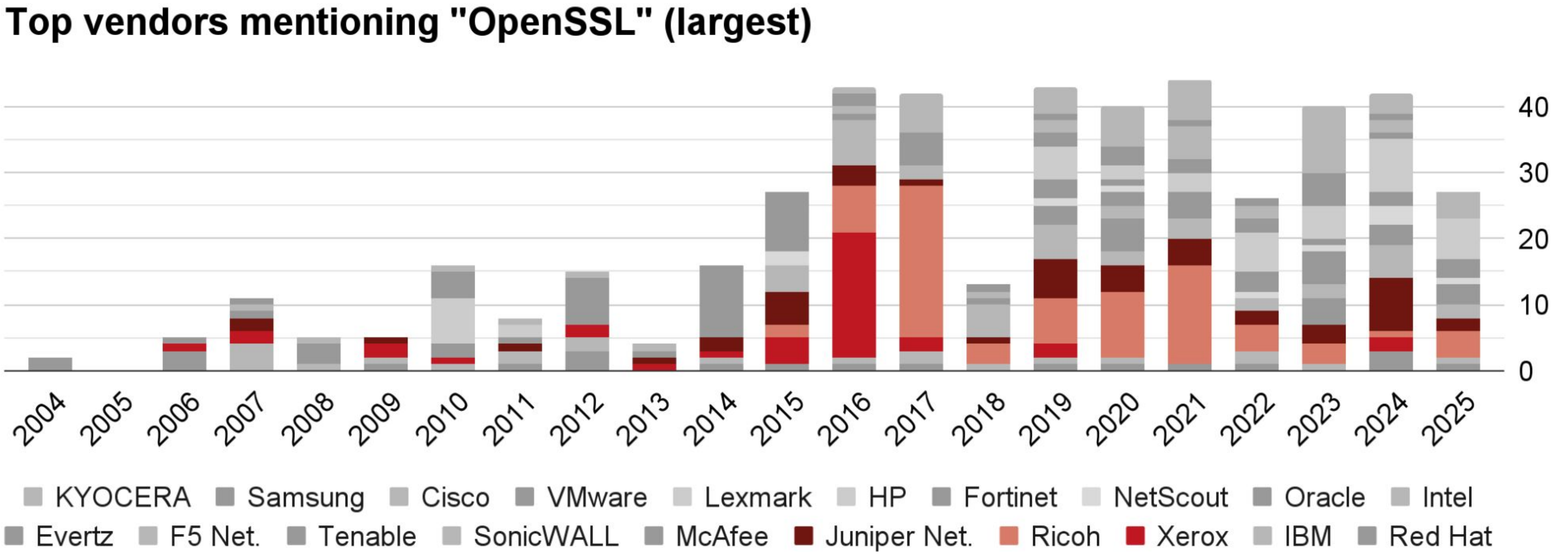
Who uses OpenSSL in their certified products?

- **313 distinct vendors mention OpenSSL** is their CC certificates
  - For comparison: There are 1 124 vendors in the CC dataset
  - Only 46 vendors (~15%) have 5+ certificates



Who uses OpenSSL in their certified products?

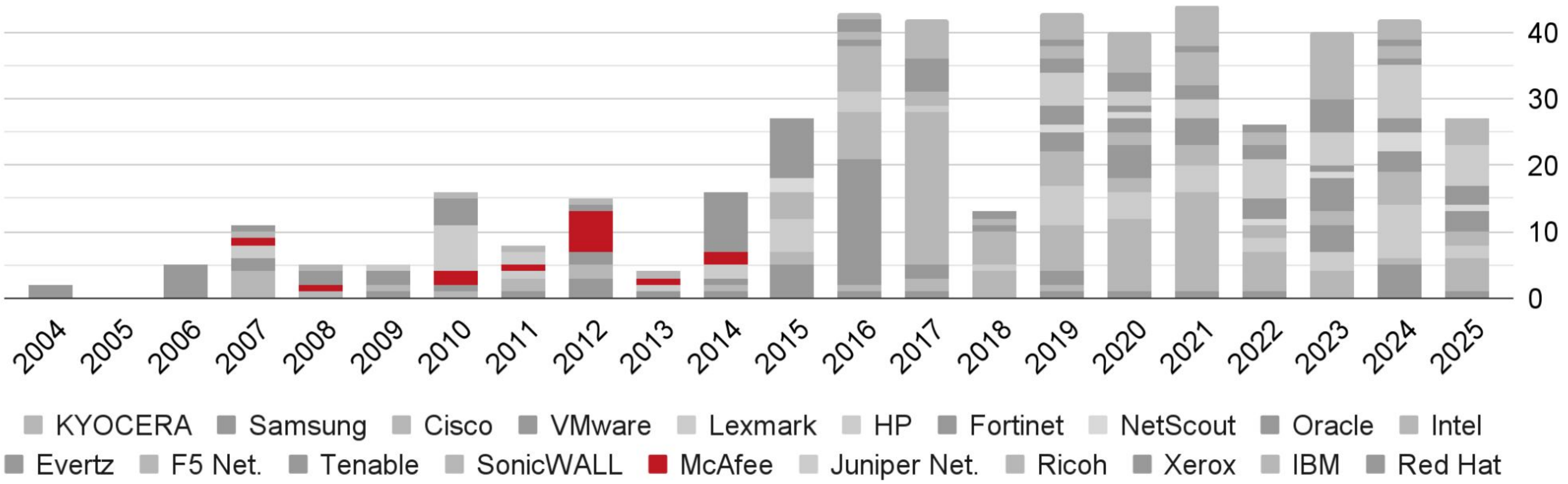
- **313 distinct vendors mention OpenSSL** is their CC certificates
    - For comparison: There are 1 124 vendors in the CC dataset
    - Only 46 vendors (~15%) have 5+ certificates



Who uses OpenSSL in their certified products?

- **313 distinct vendors mention OpenSSL** is their CC certificates
  - For comparison: There are 1 124 vendors in the CC dataset
  - Only 46 vendors (~15%) have 5+ certificates

Top vendors mentioning "OpenSSL" (discontinued)



Which alternatives are used in cert. products?

Which alternatives are used in cert. products?

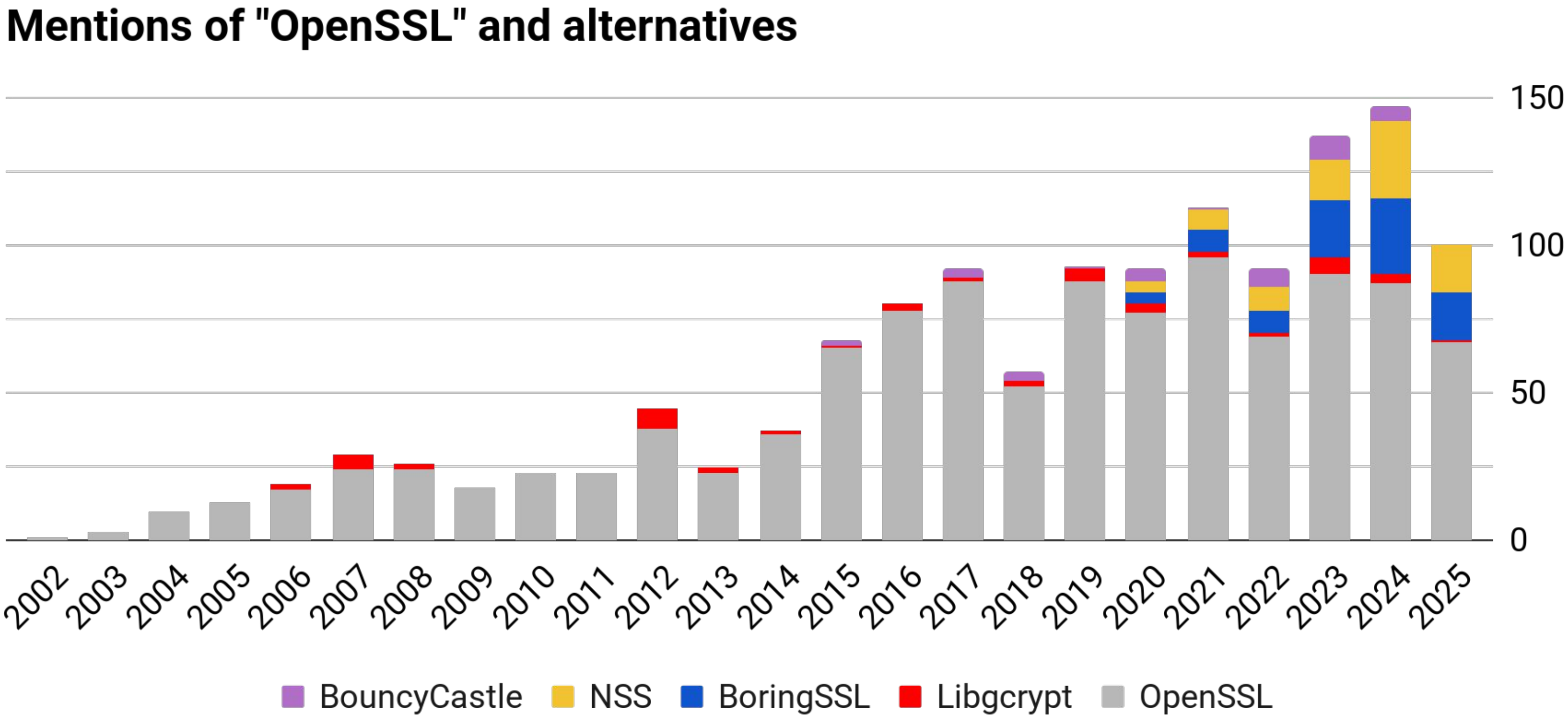
- Aspect 1: OpenSSL fork mentions
  - **BoringSSL: 80 certificates** (many Android devices)
  - LibreSSL: 2 certificates (*“due to OpenBSD base”*)
  - AmiSSL, QuicTLS, AWS-LC: no mentions

Which alternatives are used in cert. products?

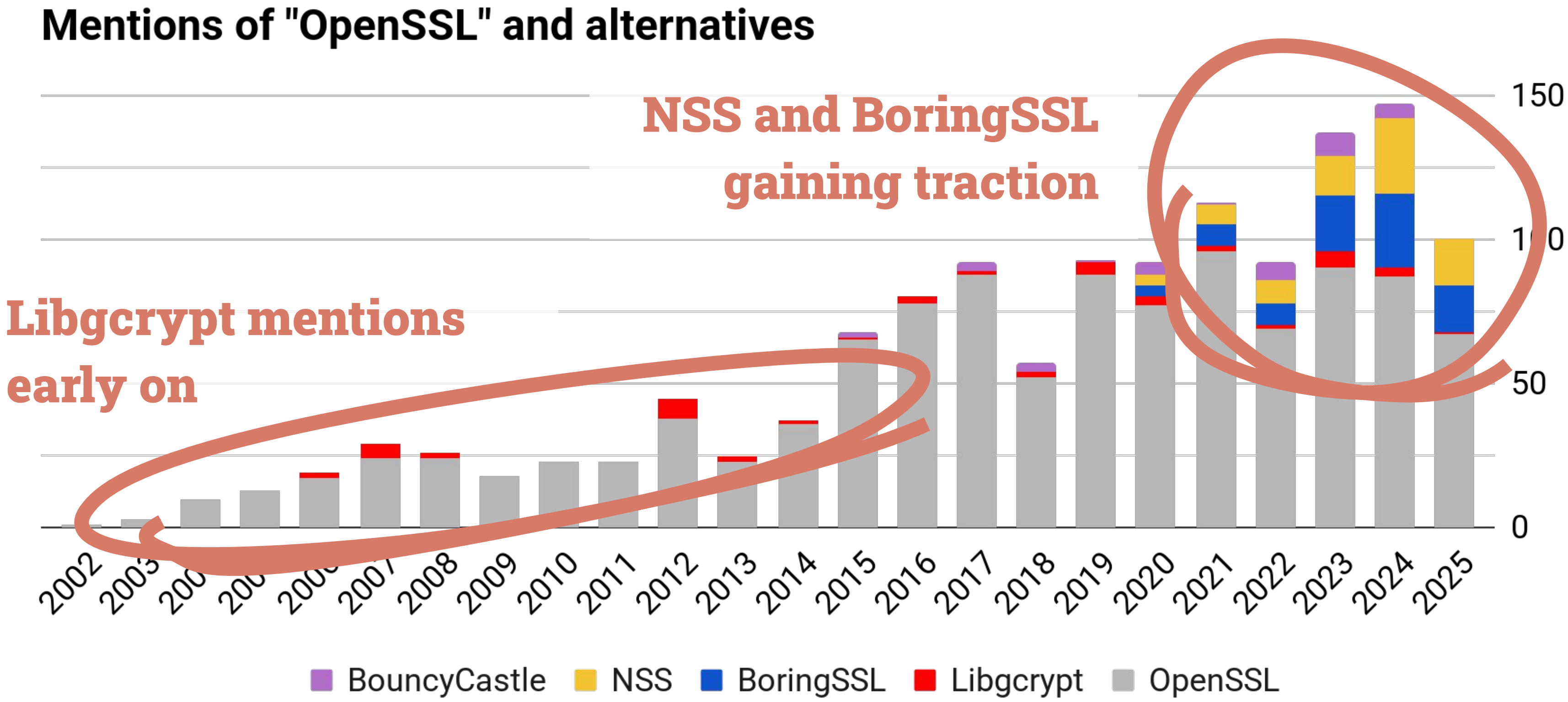
- Aspect 1: OpenSSL fork mentions
  - **BoringSSL: 80 certificates** (many Android devices)
  - LibreSSL: 2 certificates (*“due to OpenBSD base”*)
  - AmiSSL, QuicTLS, AWS-LC: no mentions

- Aspect 2: OpenSSL competition
  - **Network Security Services (NSS): 74 certificates** (RH, IBM, …)
  - **Libgcrypt: 45 certificates** (RH, SUSE, Oracle, …)
  - **Bouncy Castle: 33 certificates**
  - WolfSSL, MS crypto API, MatrixSSL, mbedTLS, Crypto++, GnuTLS, Botan: <10 certificates
  - PolarSSL, Cryptlib, GNU crypto: no mentions

Which alternatives are used in cert. products?



Which alternatives are used in cert. products?



NSS and BoringSSL gaining traction

Libgcrypt mentions early on

Part 4: Insights from FIPS 140

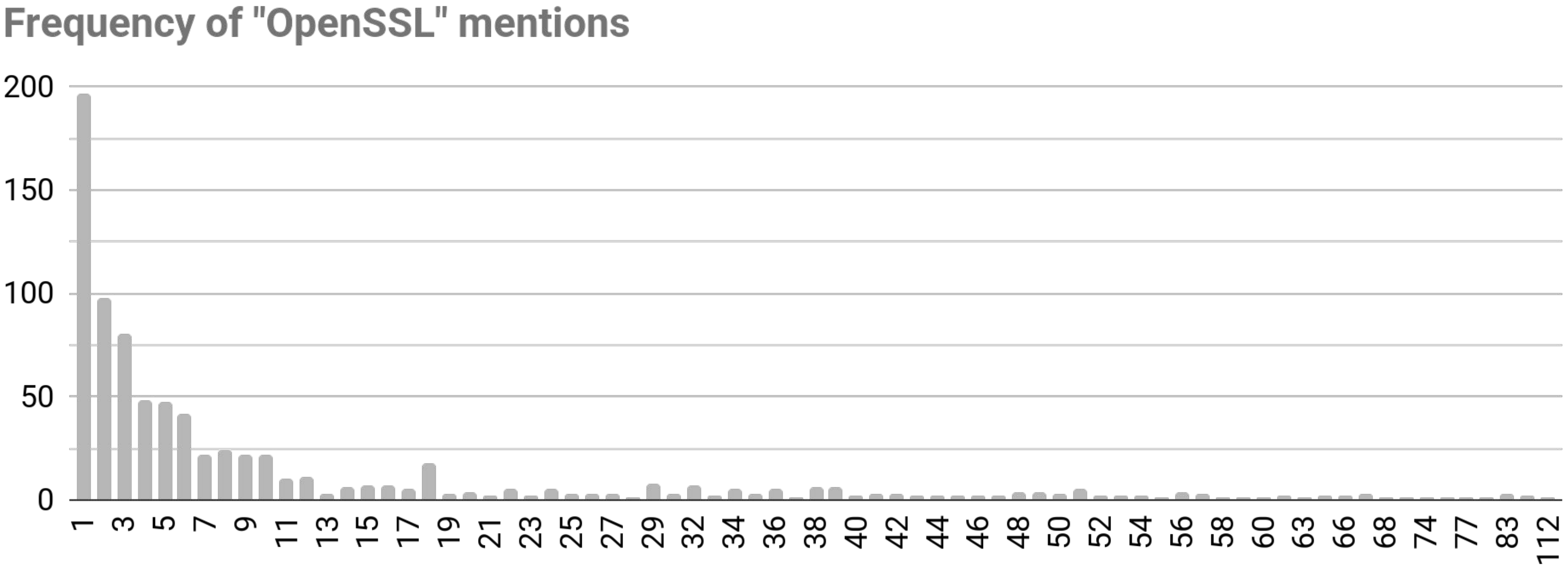
How prevalent is OpenSSL in certified products?

How prevalent is OpenSSL in certified products?

- **OpenSSL is mentioned 9 518 times** in public FIPS 140 certification files
    - For comparison: There are 5 049 FIPS 140 certificates

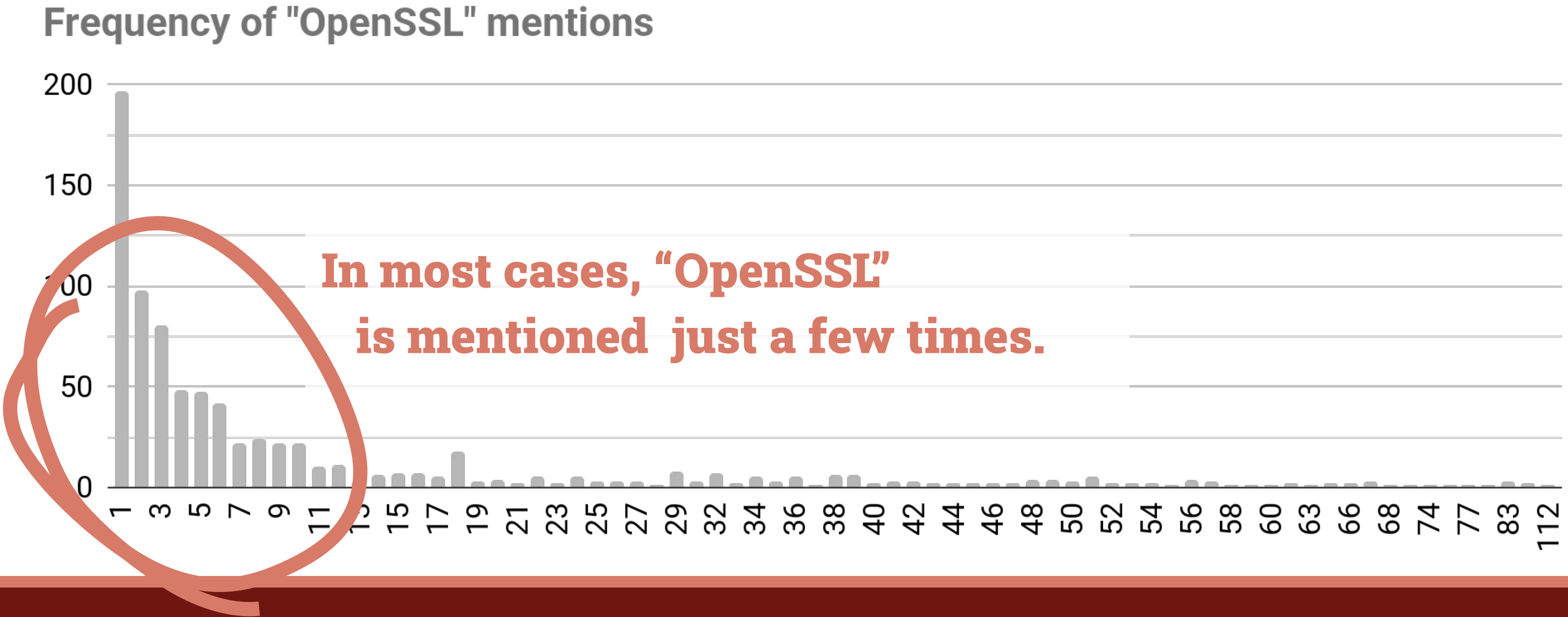
How prevalent is OpenSSL in certified products?

- **OpenSSL is mentioned 9 518 times** in public FIPS 140 certification files
  - For comparison: There are 5 049 FIPS 140 certificates



How prevalent is OpenSSL in certified products?

- **OpenSSL is mentioned 9 518 times** in public FIPS 140 certification files
  - For comparison: There are 5 049 FIPS 140 certificates



Frequency of "OpenSSL" mentions

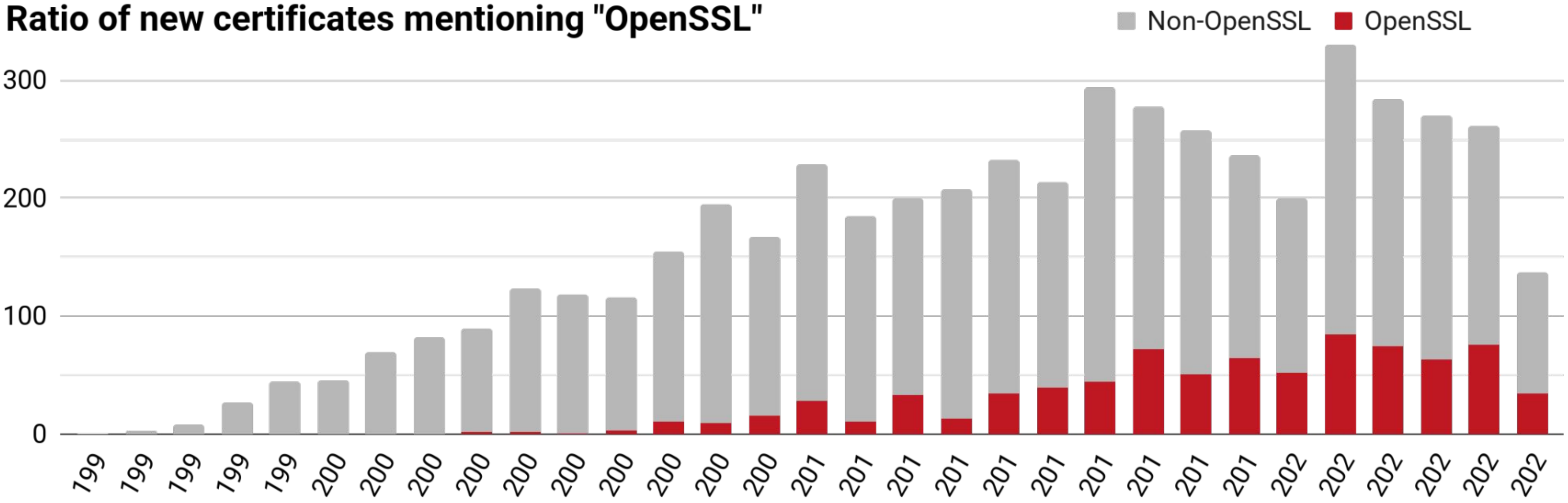
In most cases, “OpenSSL” is mentioned just a few times.

How prevalent is OpenSSL in certified products?

- **OpenSSL is mentioned in 819 distinct FIPS 140 certificates (~16%)**
  - For comparison: There are 5 049 FIPS 140 certificates

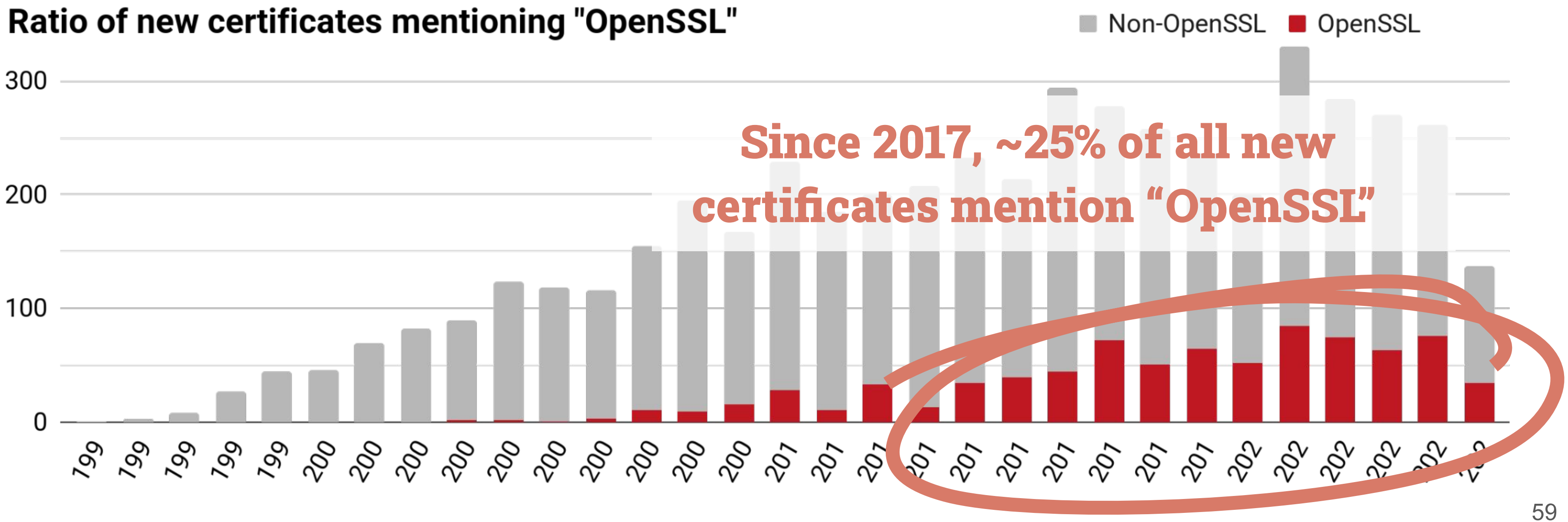
How prevalent is OpenSSL in certified products?

- **OpenSSL is mentioned in 819 distinct FIPS 140 certificates (~16%)**
  - For comparison: There are 5 049 FIPS 140 certificates



How prevalent is OpenSSL in certified products?

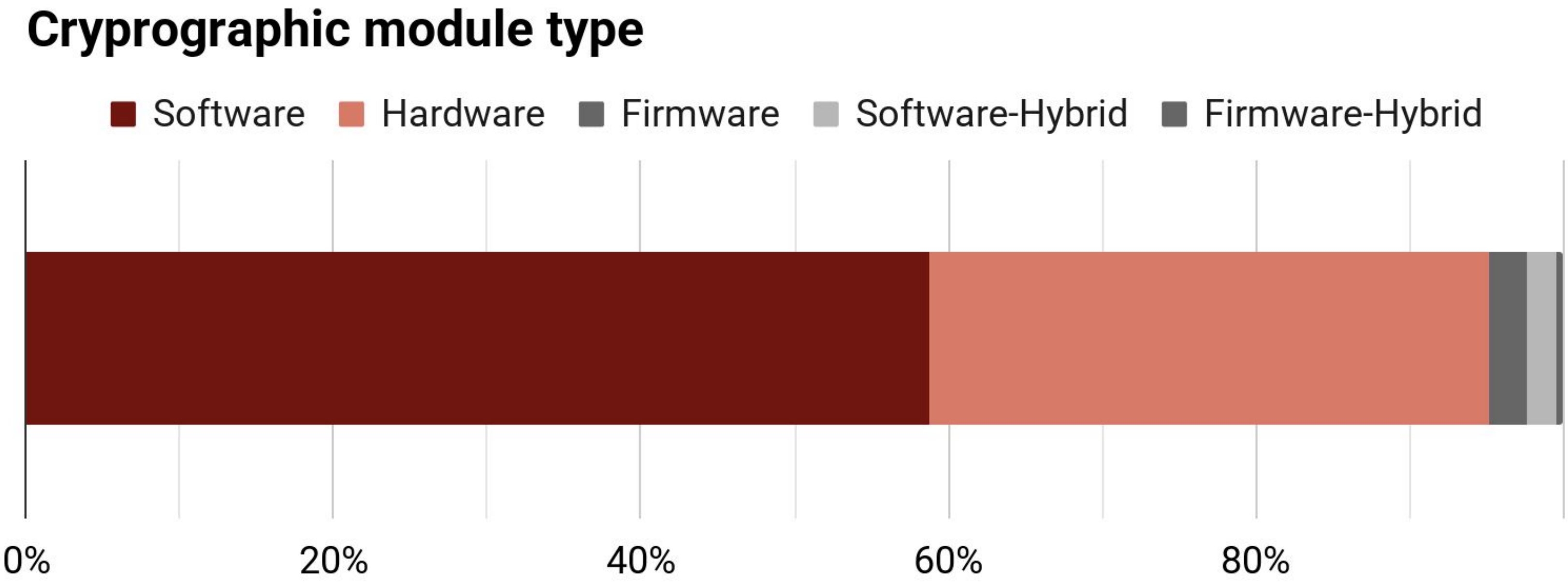
- **OpenSSL is mentioned in 819 distinct FIPS 140 certificates (~16%)**
  - For comparison: There are 5 049 FIPS 140 certificates



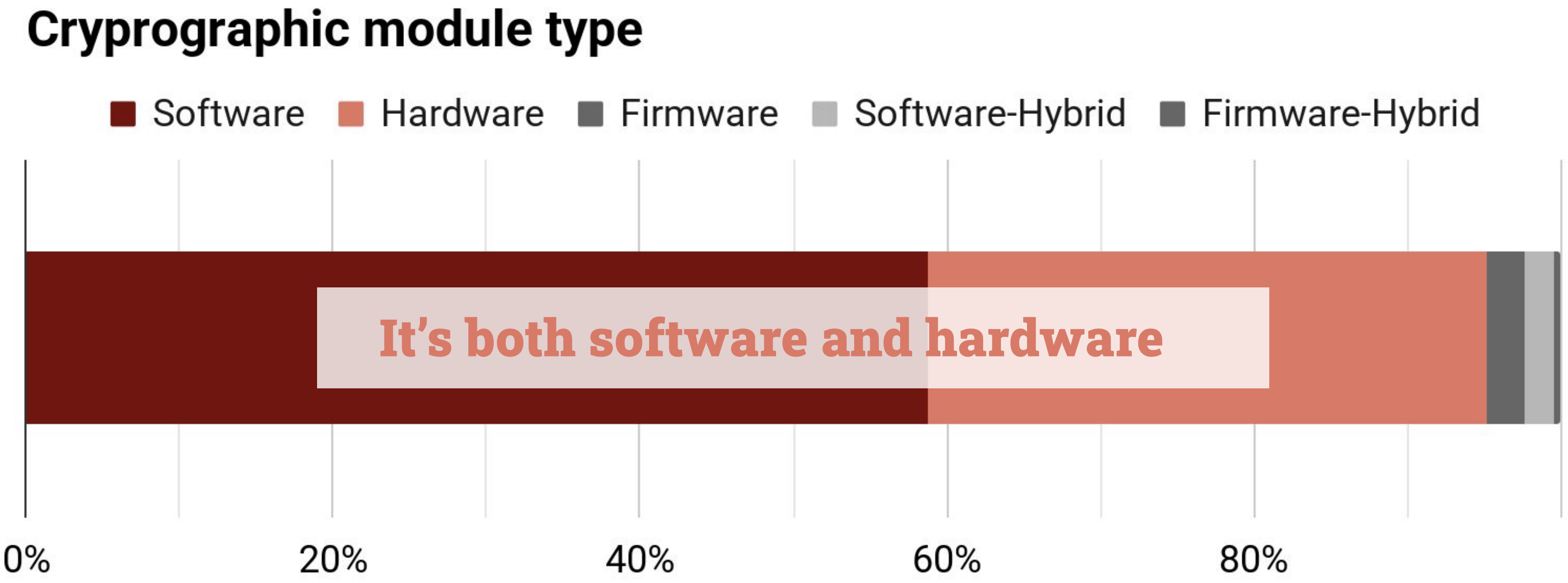
Since 2017, ~25% of all new certificates mention "OpenSSL"

What kind of certified products use OpenSSL?

What kind of certified products use OpenSSL?



What kind of certified products use OpenSSL?



It's both software and hardware

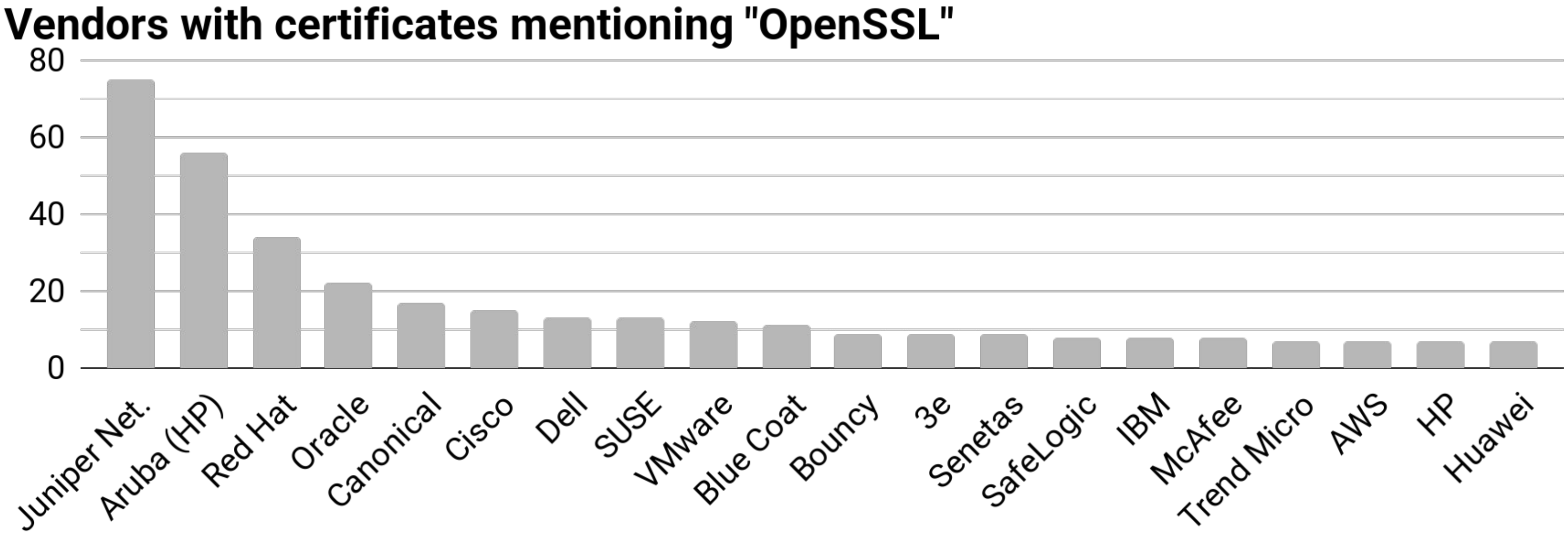
Who uses OpenSSL in their certified products?

Who uses OpenSSL in their certified products?

- **291 distinct vendors mention OpenSSL** in FIPS 140 certificates (~27%)
  - For comparison: There are 1 064 vendors in the FIPS 140 dataset
  - Only 34 vendors (~11.5%) have 5+ certificates

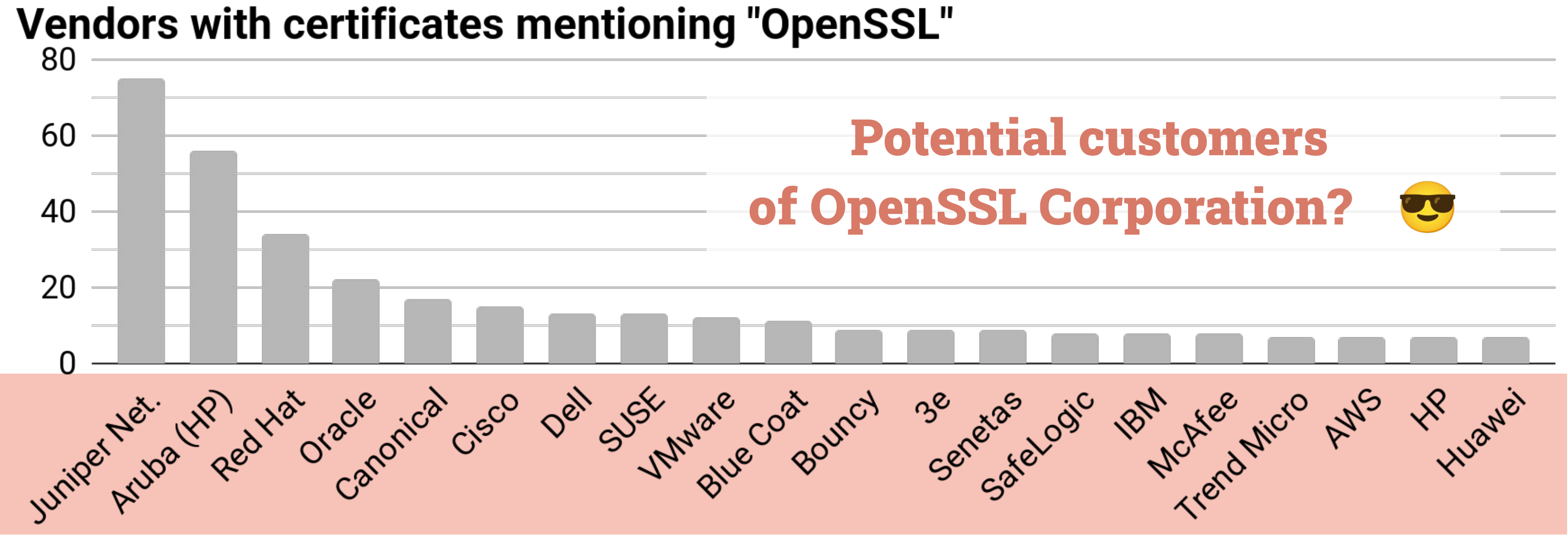
Who uses OpenSSL in their certified products?

- **291 distinct vendors mention OpenSSL** in FIPS 140 certificates (~27%)
  - For comparison: There are 1 064 vendors in the FIPS 140 dataset
  - Only 34 vendors (~11.5%) have 5+ certificates



Who uses OpenSSL in their certified products?

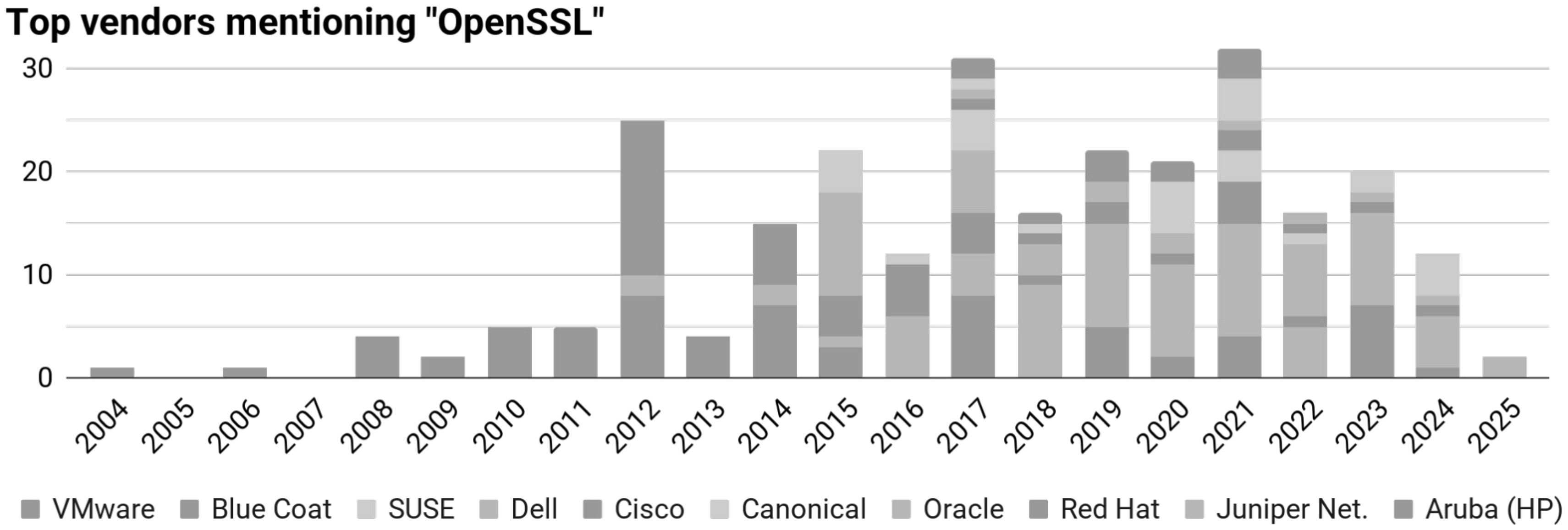
- **291 distinct vendors mention OpenSSL** in FIPS 140 certificates (~27%)
    - For comparison: There are 1 064 vendors in the FIPS 140 dataset
    - Only 34 vendors (~11.5%) have 5+ certificates


Vendors with certificates mentioning "OpenSSL"

Potential customers of OpenSSL Corporation? 😎

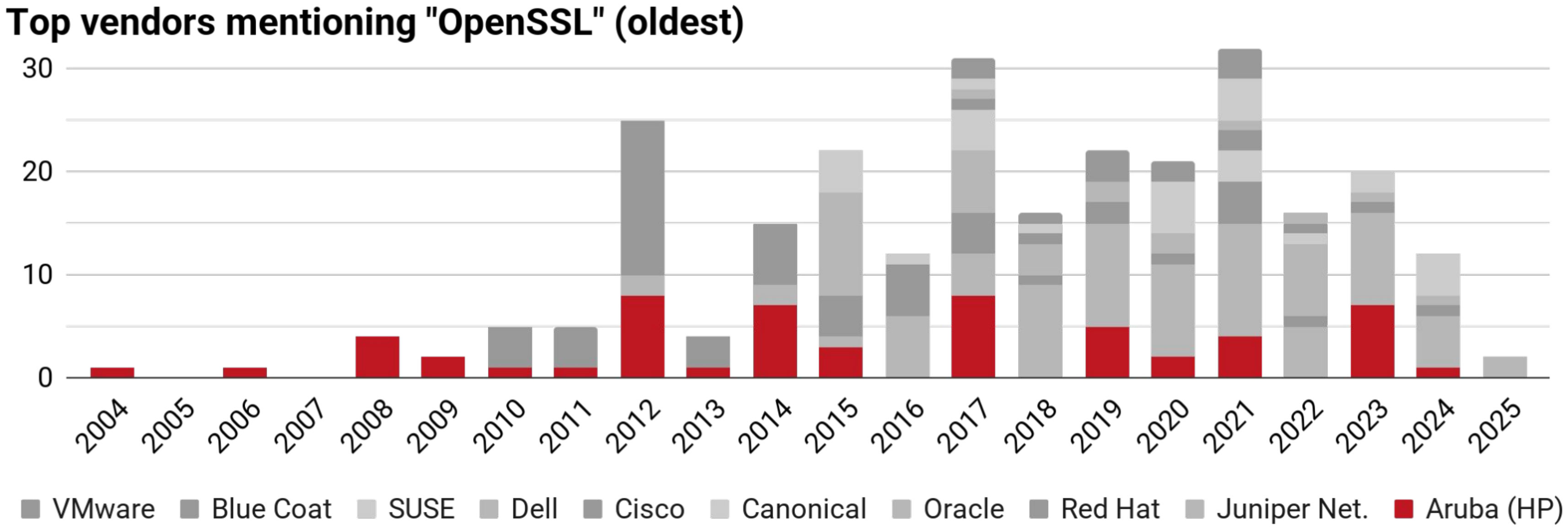
Who uses OpenSSL in their certified products?

- **291 distinct vendors mention OpenSSL** in FIPS 140 certificates (~27%)
  - For comparison: There are 1 064 vendors in the FIPS 140 dataset
  - Only 34 vendors (~11.5%) have 5+ certificates



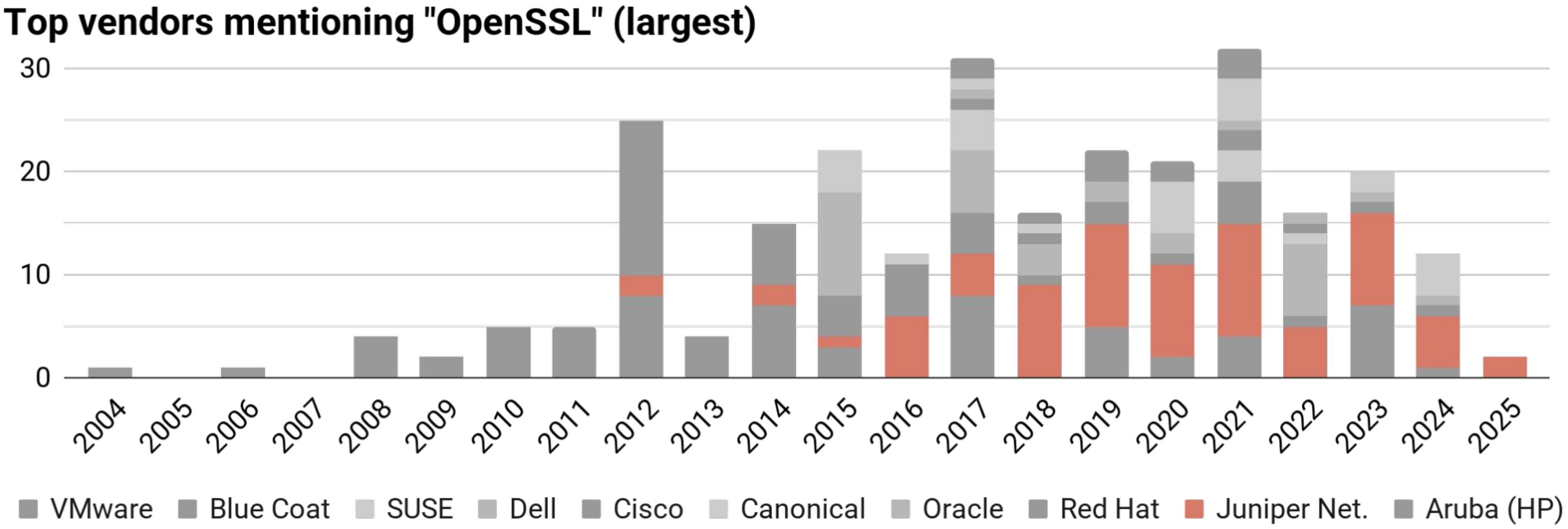
Who uses OpenSSL in their certified products?

- **291 distinct vendors mention OpenSSL** in FIPS 140 certificates (~27%)
  - For comparison: There are 1 064 vendors in the FIPS 140 dataset
  - Only 34 vendors (~11.5%) have 5+ certificates



Who uses OpenSSL in their certified products?

- **291 distinct vendors mention OpenSSL** in FIPS 140 certificates (~27%)
  - For comparison: There are 1 064 vendors in the FIPS 140 dataset
  - Only 34 vendors (~11.5%) have 5+ certificates



Which alternatives are used in cert. products?

- Aspect 1: OpenSSL fork mentions
    - **BoringSSL: 57 certificates**
    - AWS-LC: 3 certificates
    - LibreSSL, AmiSSL, QuicTLS: no mentions

Which alternatives are used in cert. products?

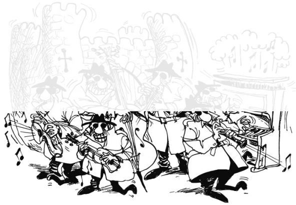
- Aspect 1: OpenSSL fork mentions
  - **BoringSSL: 57 certificates**
  - AWS-LC: 3 certificates
  - LibreSSL, AmiSSL, QuicTLS: no mentions

- Aspect 2: OpenSSL competition
  - **Network Security Services (NSS): 109 certificates**
  - **Libgcrypt: 39 certificates**
  - **Bouncy Castle: 25 certificates**
  - **GnuTLS (Nettle): 21 certificates**
  - WolfSSL, MS crypto API, Crypto++, Cryptlib, MatrixSSL, mbedTLS: <15 certificates
  - PolarSSL, Botan, GNU crypto: no mentions

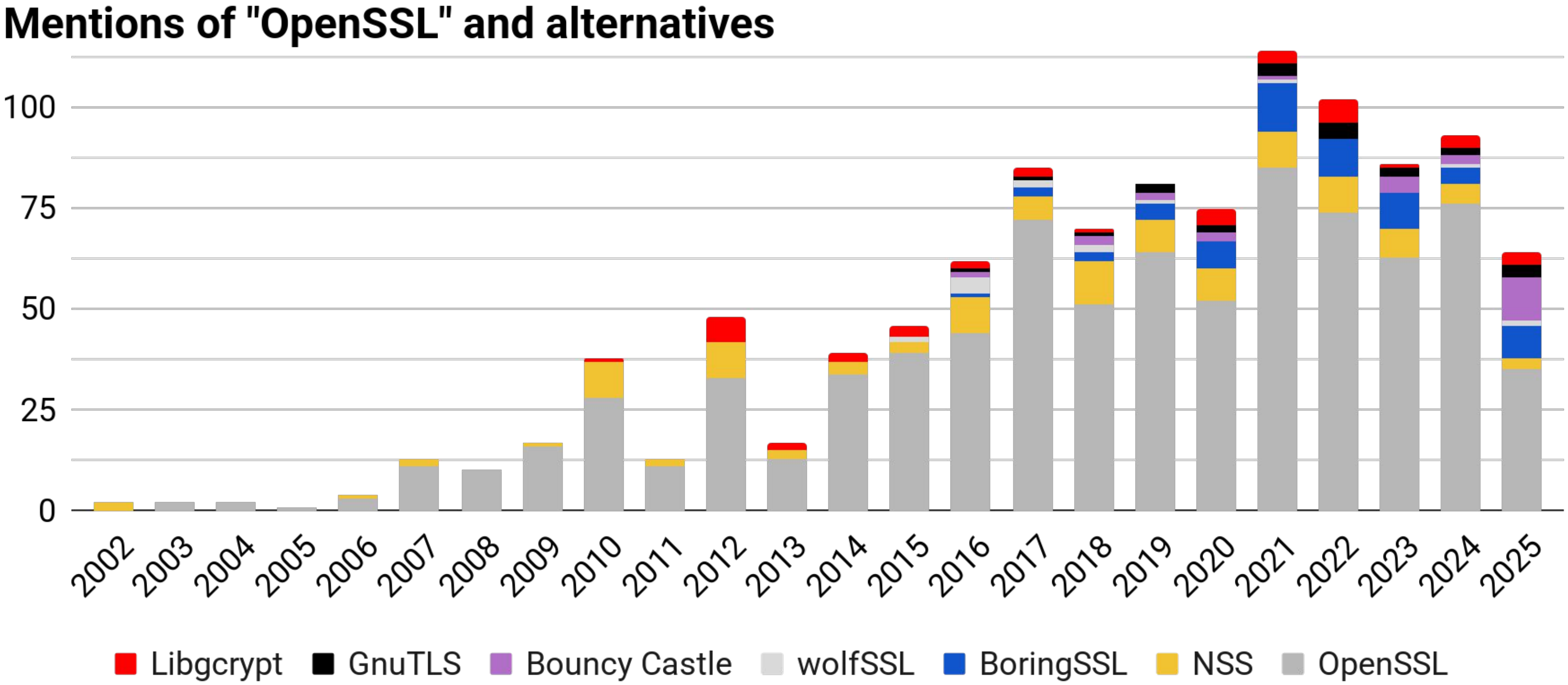
Which alternatives are used in cert. products?

- Aspect 1: OpenSSL fork mentions
    - **BoringSSL: 57 certificates**
    - AWS-LC: 3 certificates
    - LibreSSL, AmiSSL, QuicTLS: no mentions
- Aspect 2: OpenSSL competition
    - **Network Security Services (NSS): 109 certificates**
    - **Libgcrypt: 39 certificates**
    - **Bouncy Castle: 25 certificates**
    - **GnuTLS (Nettle): 21 certificates**
    - WolfSSL, MS crypto API, Crypto++, Cryptlib, MatrixSSL, mbedTLS: <15 certificates
    - PolarSSL, Botan, GNU crypto: no mentions

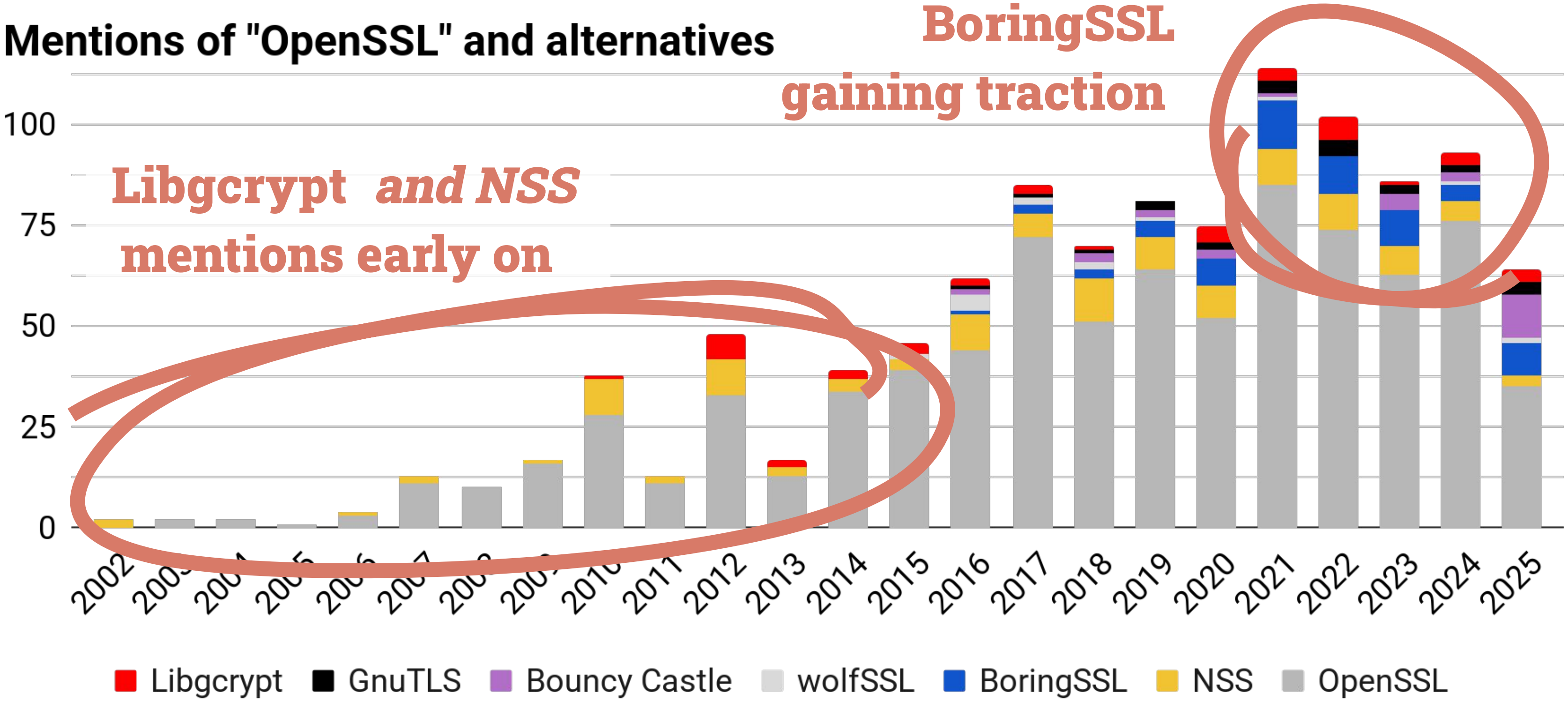
Same story as CC
(just GnuTLS more prominent)



Which alternatives are used in cert. products?



Which alternatives are used in cert. products?



BoringSSL gaining traction

Libgcrypt *and NSS* mentions early on

Part 5: Conclusions

Summary

- **sec-certs.org as a unified API over public CC/FIPS 140 documents**
- To get unseen insights about OpenSSL (or other product)

Summary

- **sec-certs.org as a unified API over public CC/FIPS 140 documents**
- To get unseen insights about OpenSSL (or other product)

- OpenSSL is a really significant player in crypto libraries

Summary

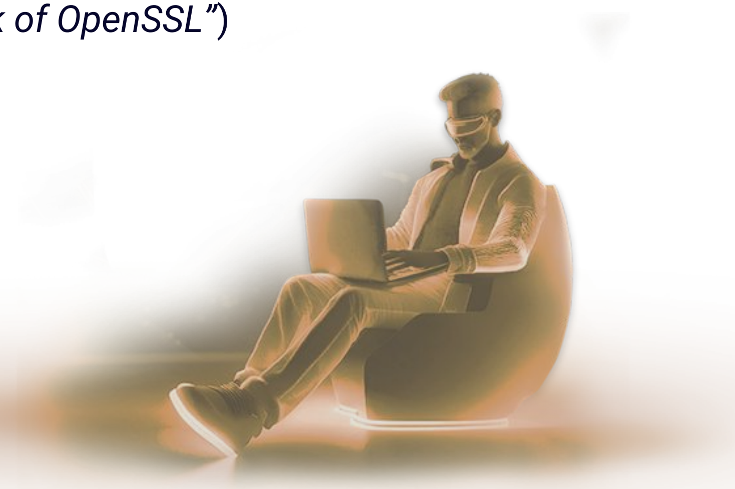
- **sec-certs.org as a unified API over public CC/FIPS 140 documents**
- To get unseen insights about OpenSSL (or other product)

- OpenSSL is a really significant player in crypto libraries
- But having data is different to having a gut feeling!

- In last 10 years, **~every fourth certificate mentions OpenSSL**
- **~quarter of vendors mentioned OpenSSL** in at least one certificate
- NSS, BoringSSL, Libgcrypt are the most common alternatives
- The situation in CC and FIPS 140 ecosystems is very similar

Limitations and biases

- Dataset deficiencies
  - Broken PDFs, failed OCR, non-English content, …
- Parsing imperfections
  - Semantics ignored (*“Uses BoringSSL which is a fork of OpenSSL”*)
  - Heuristics and metadata consolidation
- Differentiating certificates vs. products
  - Certificate renewals, product versions, …



Limitations and biases

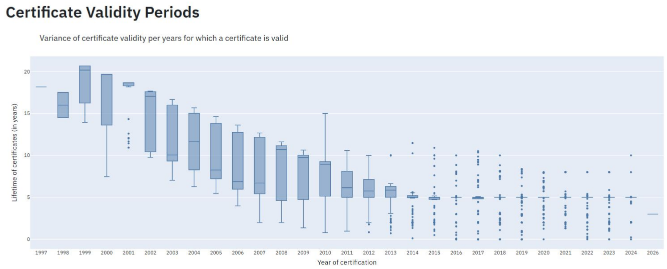
- Dataset deficiencies
  - Broken PDFs, failed OCR, non-English content, …
- Parsing imperfections
  - Semantics ignored (*“Uses BoringSSL which is a fork of OpenSSL”*)
  - Heuristics and metadata consolidation
- Differentiating certificates vs. products
  - Certificate renewals, product versions, …
- **Only certified products/modules**

Extensions

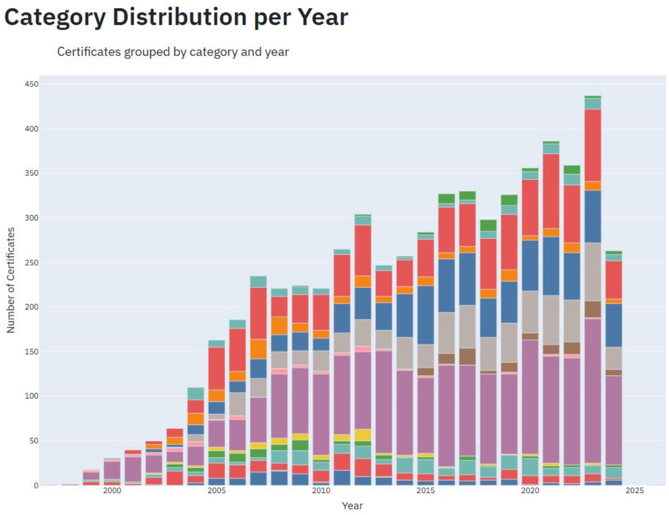
sec-certs

Other interesting data can be mined:

- Deeper product/component analyses
  ("Which OpenSSL versions are in active certificates?")
- Comparing certification labs
  ("Was lab XY doing smart cards lately?")
- Getting ecosystem stats
  ("How long does it take to pass the FIPS 140 certification?")
- Security analysis
  (certificate dependencies, linking through CPEs to CVEs, misconfigurations and deprecated crypto in certified products)


Certificate Validity Periods

Variance of certificate validity per years for which a certificate is valid


Category Distribution per Year

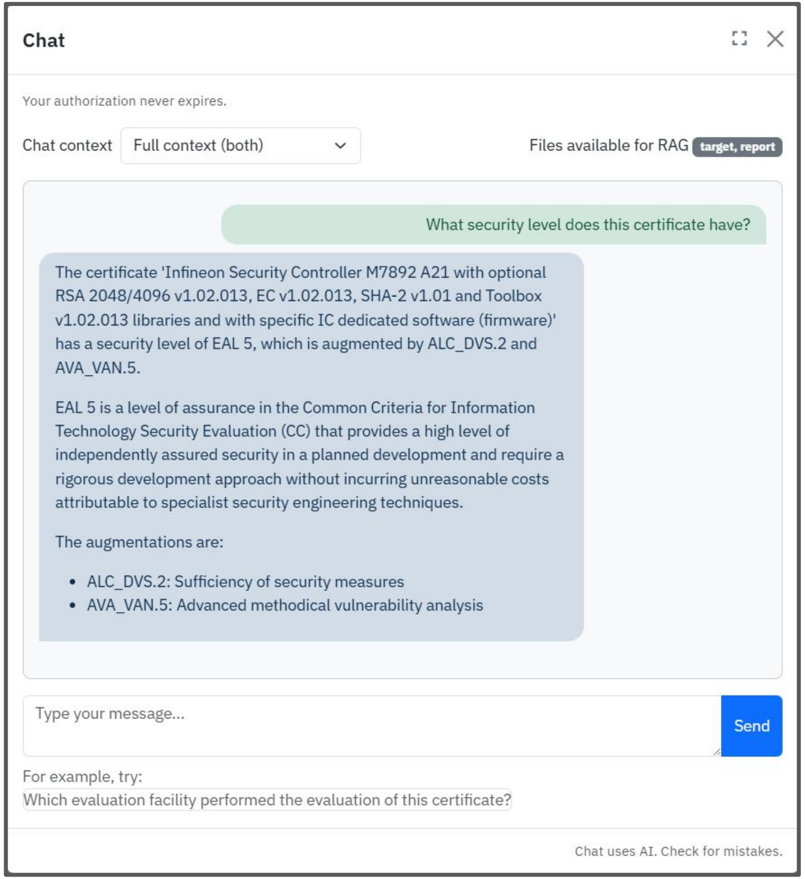
Certificates grouped by category and year

Obvious extension

- Use LLMs to chat with certification documents
- Already in progress (closed beta)

Want to chat with certificates?

https://sec-certs.org/



Your authorization never expires.

Chat context: Full context (both)

Files available for RAG: target, report

What security level does this certificate have?

The certificate 'Infineon Security Controller M7892 A21 with optional RSA 2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware)' has a security level of EAL 5, which is augmented by ALC_DVS.2 and AVA_VAN.5.

EAL 5 is a level of assurance in the Common Criteria for Information Technology Security Evaluation (CC) that provides a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.

The augmentations are:

- ALC_DVS.2: Sufficiency of security measures
- AVA_VAN.5: Advanced methodical vulnerability analysis

For example, try:
Which evaluation facility performed the evaluation of this certificate?

Chat uses AI. Check for mistakes.

What next? (Actionables)

- Search for your products at **sec-certs.org**
- Search for your competition at **sec-certs.org** 😁

What next? (Actionables)

- Search for your products at **sec-certs.org**
- Search for your competition at **sec-certs.org** 😁

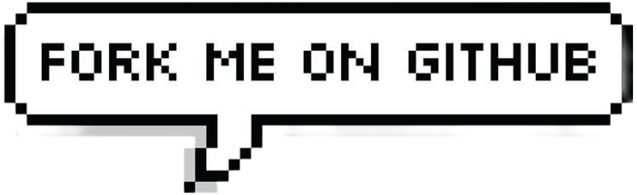
- Fork the repo, download the public dataset, perform custom deeper analyses
    - And let us know what is useful for people!

FORK ME ON GITHUB

What next? (Actionables)

- Search for your products at **sec-certs.org**
- Search for your competition at **sec-certs.org** 😁

- Fork the repo, download the public dataset, perform custom deeper analyses
  - And let us know what is useful for people!



- Interested in research side of sec-certs? ***Get in touch!***
- Interested to push transparency in certifications? ***Get in touch!***
- Willing to support this university project? ***Get in touch!***
  - (money, developer time, resources, …)

Thank you + Q&A

- Use sec-certs.org to get insights
    - About products
    - About components/configurations/…
    - About certification ecosystem
- Get in touch to discuss your use case
- Get involved and collaborate

MASARYK UNIVERSITY

Co-funded by the European Union

CHESS

Red Hat

sec-certs

Try it on your own!

https://sec-certs.org/