Reinventing Content Disarming

Leader in Advanced Malware Prevention for Documents/Files

400+
CUSTOMERS

5BN.
DOCUMENTS PROCESSED

0
BREACHES

Votiro has a 100% prevention rate against known and zero-day attacks

Votiro's easy-to-use and effective technology positions the Company for strong growth in document/file-based malware prevention

Validated by Gartner as a must-have technology to protect against content-based threats

COMPANY OVERVIEW

- Reinventing the Content Disarm & Reconstruction Space (CDR)

Proprietary technology instantly deconstructs and reconstructs content of all types—in original file format—making it safe for enterprise use

- Improves business productivity with no user action and insignificant latency—and zero malicious files entering the network
- Protected by 15+ US patents covering multiple core techniques
- Founded in Israel, with sales presence in the US, Israel, APAC, and Australia

MARKET OPPORTUNITY

- The most virulent malware, like ransomware, is zero-day and hidden in files
- Uploading and downloading files are a business necessity
  - *No other platform is both Zero Trust based and 100% effective*
  - *No other security technology preserves all the content and embedded content in its original file formatting—ready for business operations*
  - *Cloud and web based architectures don't eliminate the risk of uploading and downloading malicious content*
- $1.3B annual addressable market
  - *Complementary technology to virtually all other state-of-the-art security layers (web gateway, email gateway, content services, identity and access management, CASB)*

By 2022, Gartner expects 20% of organizations to use CDR as part of their content protection strategies

SOLUTION / VALUE

- Improves businesses' ability to collaborate online safely, enhancing productivity
- Operational and compliance peace of mind; all users can open any document without concern, risk, or extra user action
- Votiro technology can be integrated into any content-based application from all communication channels, including encrypted files…with no file security gaps
- Very low TCO
  - *No user training*
  - *Graceful integration with existing security infrastructure*
  - *Virtual – in the cloud or on prem*
- Rapid ROI
  - *No security breaches by content born malware*
  - *Reduced incident response staff workload*
  - *More network visibility with an easy to use management console*
- Sustainable technology advantage of patents, know-how, and track record
- Proven market leader of content security at large Enterprise scale

GO-TO-MARKET STRATEGY

- Focus on building direct and channel sales resources, going after enterprises, financial services, and government sectors
- Build on Votiro's rapid sales growth in the US
- Extend significant presence in APAC boosted by regulation and guidelines
- Leverage strong and increasing pipeline of *Fortune 2000* companies
- Expand on major technology integration partnerships

FINANCIAL PROFILE

- 125% Bookings growth forecast for 2020; >$5M in orders
- 27 employees
- Subscription business model (since 2019)
- Cash flow positive Q1 2022
- Capital raised to-date: $14M

This raise: $5M for accelerated sales expansion and roadmap execution

EXAMPLE REFERENCE ACCOUNTS

- Large US financial services company; processes billions of dollars worth of digital loan applications through an upload portal
- Large APAC bank with 300,000 email users requiring document security
- US Health Insurance network with large number of email users and online claims via its portal
- US investment firm; securing downloads from the web

Votiro succeeds where CDR has not.

Now scheduling calls for interested parties that want to know more

VOTIRO CONTACT

Chris Fedde | **chris.fedde@votiro.com**

Rev. 4/9/2020

EXECUTIVE SUMMARY

March 2020

THE COMPANY

- **Votiro** reinvented Content Disarming & Reconstruction (CDR) as a cyber threat prevention against content-born attacks, establishing a **Secure File Gateway** category
- **Votiro** has a proven prevention rate of 100% against both known & unknown (e.g. zero-day) attacks
- **Votiro** improves business productivity for organizations of all sizes by delivering content in original formatting, ready to use, with no user action—& free of malware…providing operational peace of mind, allowing users to click on any file without the need to think twice
- **Votiro's Positive Selection™** technology consistently & substantially outperforms CDR solutions, with no dependence on finding or countering hidden malware
- **Votiro's Secure File Gateway** can be gracefully integrated with any content-based application from all communication channels, including encrypted files…no file security gaps
- High quality, demanding customers—particularly in banking & finance, insurance, technology & telecoms—with strong pipeline
- Subscription model with sustainable price points & high product margins

- Founded in Israel in 2012; first product shipped in 2014
- Sales presence in the US, APAC, Israel & Australia; HQ moving to the US
- Expect 140% growth of subscription orders to $5.5m in 2020
- 2020 US growth >300%; $125k ADS track record
- Over 400 customers, ranging from <500 users to >300,000 users
- Over 5 billion documents processed; zero breaches
- 15 US patents
- Experienced Management Team
- $14m seed invested (all Common); $5m Series A underway (Preferred)

VOTIRO SECURED.

VOTIRO SECURE FILE GATEWAY PLATFORM

At a glance

Documents & files are a business necessity

- They enter through many sources
  - Web
  - Email
  - Collaboration
  - Custom business applications
  - SMB/FTP shares
  - Help Desk *(e.g., ServiceNow, Salesforce)*
  - EFSS/CCP *(e.g., Dropbox, Box)*
- They can hide a full spectrum of malware

VOTIRO SECURED.

Delivering Safe Content in Milliseconds

1 *Analyze*

- Disassemble into objects
- Analyze sections, macros & metadata
- Non-harmful parts extracted

2 *Reconstruct*

- Reconstruct a 100% Known-Safe version
- Reconstruct full depth of macros

3 *Test*

- Automated Fidelity Test

4 *Deliver*

- Deliver in original source formats
- Full functionality

WHAT WAS CDR SUPPOSED TO DO?

Objective: Threat Prevention

- Cyber threats that aren't *prevented* get into the network. They result in compromise and cost, sometimes staggering cost.
- All threat *prevention* requires that the threats be found—identified—before they get into the network. This is the cyber arms-race of cyber products trying to keep up with the threats

Why CDR?

- The most virulent attacks, including zero day and ransomware, are delivered by hiding the attacks in content—the content that is essential to business (documents, files, attachments…).
- CDR was envisioned to *prevent* threats by neutralizing them and reconstructing the content to be safe before it gets to the network.

The Problem:

- Traditional CDR still relies on finding the potential threat in the content, removing parts of the content, or else converting the content to a different format—thus rendering it unsuitable for its intended business use.
- Traditional CDR technology didn't faithfully, reliably reconstruct content in a known-safe condition.

VOTIRO SECURED.

SOLUTION: POSITIVE SELECTION
SUCCEEDING WHERE CDR DIDN'T

Votiro's Newly Developed Technologies that:

- Reconstruct new, **known-safe** content…
  - In original formatting…
    - Ready for safe business operations…
      - Without having to find, alter, or remove malware hidden in the original content.

Operational Peace of Mind for:

- Email
- File Sharing
- Document Portals
- Help Desks
- Enterprise File Synchronization
- Websites
- Collaboration
- Business Applications, ERP, CRM

VOTIRO SECURED.

PROPOSED TRANSACTION

Opportunity

The promise and the power of Content Disarm and Reconstruction (CDR) was always obvious – delivering usable known-safe content. First generation CDR didn't deliver on that promise. First gen technologies required the capability of discovering hidden malware, or changing or removing some content-critical elements, neither of which leads to usable known-safe content.

In 2012 Votiro's research created true next generation technologies that could reconstruct content of all formats into safe content of the original format. Further, it requires no knowledge of what potential malicious code may be hidden in the original content. After two years of development Votiro used their new, patented IPR to win the large government mandated cyber security program in Japan. Adoption and validation by the Japanese government lead to CDR wins in Singapore and Israel, making 2017 Votiro's most successful year.

The years of 2018 and 2019 were transitional years for Votiro, including a CEO change, new investors and new reassembly capabilities. Along with this came a new business strategy, a change over to SaaS subscription, expanding sales in APAC and most dramatically in the US. A two person sales team in the US achieved rapid traction in 2019 with wins and PoCs with several large, sophisticated blue chip companies.

With this global validation of technology and market acceptance, including the US, the company is ready to raise additional capital and aggressively grow their business and the company valuation.

A fuller description of Votiro and the background of CDR is at the end of this document

Objective

The Company is planning expansion at all touch points of its business strategy. The capital raise will provide a runway to cash flow positive (Q1'22), with a buffer amount remaining on the balance sheet.

Capitalization to date has been $14m. The capital being raised now is $5m. The valuation of Votiro will grow dramatically in the next 12-18 months as it establishes more blue-chip wins in the US, demonstrates product superiority, and introduces new capabilities.

VOTIRO SECURED.

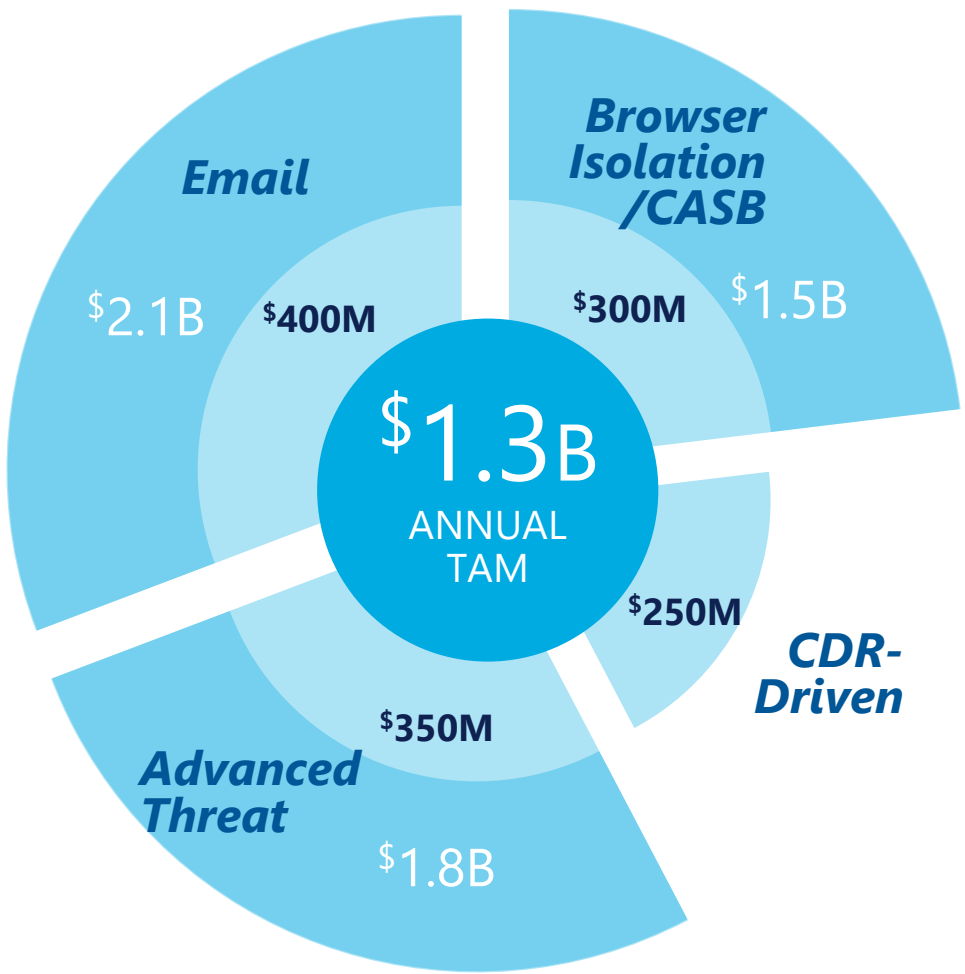
VOTIRO IS ALIGNED WITH MAJOR CYBER MARKET DRIVERS

		VOTIRO SECURED.
Prevents the Full Spectrum of Content-Borne Attacks	*The cyber threat problem is global and unrelenting.* The most virulent malware, like ransomware and zero-day is hidden in files. In addition, the sheer volume of known attacks means that they too also slip into the network hidden in content.	Stops losses due to content-borne cyber attacks
Security & High Velocity Business	*Every user action and any detectable latency interferes with today's business.* A product that delivers user-ready, *safe* content at very high speeds enhances business.	Improves business productivity; no latency
Integrates Into Existing Applications & Structure	*Stand-alone security solutions create complexity and expense.* A product that integrates with existing structures and content services, and introduces no new actions for the users or the IT staff, avoids that complexity and cost. In addition, Prevention vs Detect & Respond is a huge time saver for security staffs.	Reduces workload & increases productivity of IT/IS staffs; low TCO
Operationalizes Zero Trust	*Next generation CDR does not depend on finding and removing malware.* First-gen CDR was like other security layers in that they had to either identify attacks in order to prevent them, or remove significant parts of the document. Next-gen CDR creates known-safe content. It does not depend on knowledge of the threats.	Avoid obsolescence; no reliance on analytical or predictive technologies, intelligence, or NG/AV limitations
Cloud & Virtualized Networks	*Organizations of all sizes are optimizing infrastructure with cloud use.* Security products that are designed to run on-prem only or in cloud only can be big business obstacles as organizations migrate and/or hybridize.	Equally effective at attack prevention as a cloud or premises implementation

ADDRESSABLE MARKETS

2020 Market Focus

- Enterprise Content Services
  - Email
  - Web
  - File transfers
  - Simple integration to existing business applications
- Direct Sales
- Technology partnerships
- 300% growth in the US
- Virtual on-premises
- APIs to cloud services



By 2022, Gartner expects 20% of organizations to use CDR as part of their content protection strategies.

VOTIRO SECURED.

VOTIRO SECURE FILE GATEWAY CUSTOMER USE EXAMPLES

Customer	*Use*	*Our Edge*
Large US Financial Services Company	• Secure upload portal for consumer loans • 3,000 applications/hour • $6.4B in loans	• Fastest Content Reconstruction in the market • Scalable
Large APAC MSP	• 300,000 Users • Email • Web uploads	• Rapid Integration through API • Speed • Scalable
US Health Insurance Network	• Email • Client portal • File transfers • Web downloads	• Processes all the content types • Integrates with multiple existing systems *(e.g., GoAnywhere)* • Speed
US Multinational Investment Firm	• Web browsing • Enterprise files synch/sharing	• Processes all the content types • Tightly integrates with existing systems *(e.g., Symantec)*
Large Multinational APAC Bank	• Email infrastructure • 300,000 users & climbing • Will expand to file upload/download	• Processes all the content types • Business-ready content • Scalable

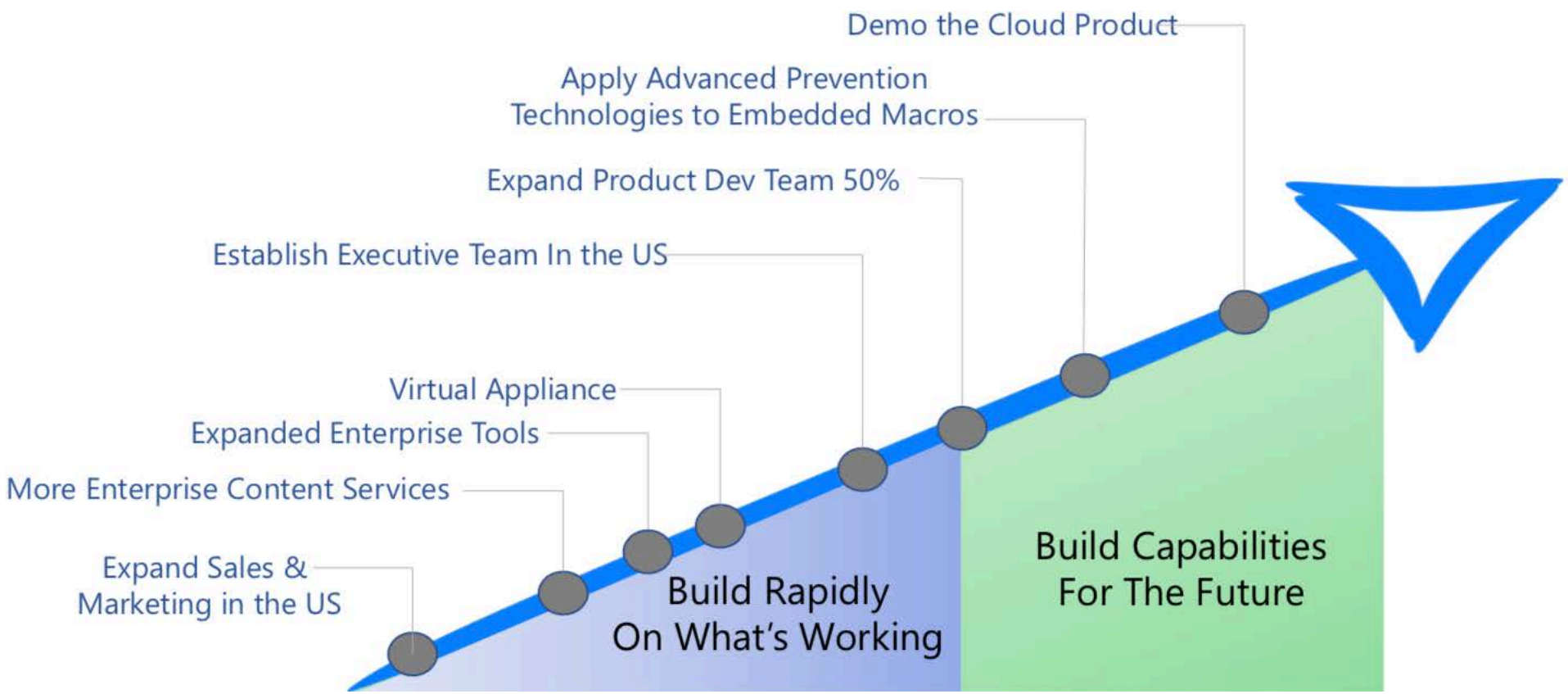
SECURED.

COMPARING COMPETITIVE TECHNOLOGIES

	VOTIRO SECURED.	*CDRs* *Glasswall/OPSWAT/ Checkpoint*	*Sandboxes*	*NG Antivirus*	*Phishing Awareness*
Relies on Finding Malware	No	No	Yes	Yes	Yes
Relies on Predictive Analysis	No	No	Yes	Yes	Yes
Delivers Fully Functional Content	Yes	No	Yes	Yes	No
Delivers Known-Good Content	Yes	No	No	No	No
Effective Against Zero Days	Yes	Sometimes	Sometimes	No	No
Affects Productivity	No	Yes	Yes	Sometimes	Yes
False Positive Rate	0	High	High	Medium	High
False Negative Rate	0	0	High	Medium	High
Maintenance	Very Low	Medium	High	Low	High
Latency	Milliseconds	Secs to Mins	Minutes	Milliseconds	–

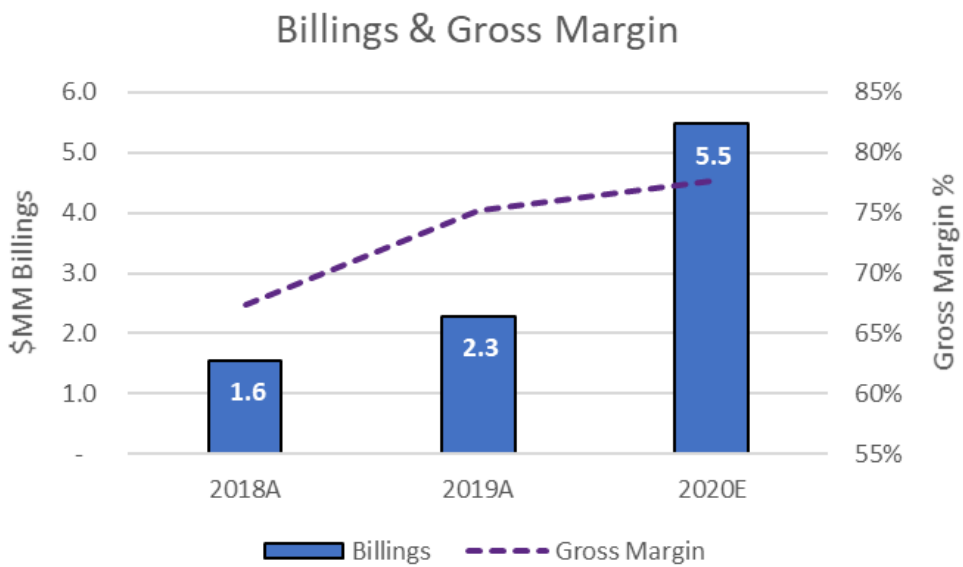
GROWTH STRATEGIES

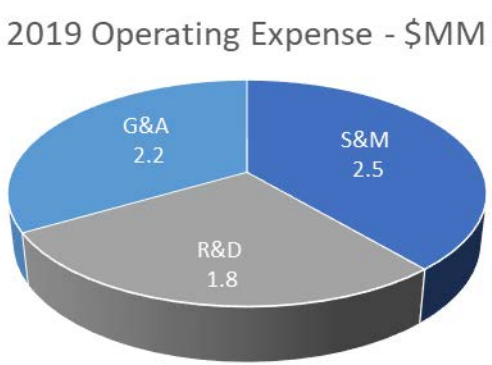
Votiro's Use of New Investment — 2020



VOTIRO SECURED.

COMPANY FINANCIALS





Income Statement

$MM	2018A	2019A	2020E
Billings	1.6	2.3	5.5
YtY%		*47%*	*139%*
Revenue	**1.9**	**2.1**	**3.1**
Gross Profit	**1.3**	**1.6**	**2.4**
Gross Margin %	*67%*	*75%*	*78%*
S&M	2.2	2.5	3.7
R&D	2.0	1.8	2.4
G&A	2.0	2.2	2.3
Operating Expense	**6.2**	**6.5**	**8.4**
Operating Income	**(4.9)**	**(4.9)**	**(6.0)**
Operating Cash-flow	(6.4)	(4.5)	(4.4)

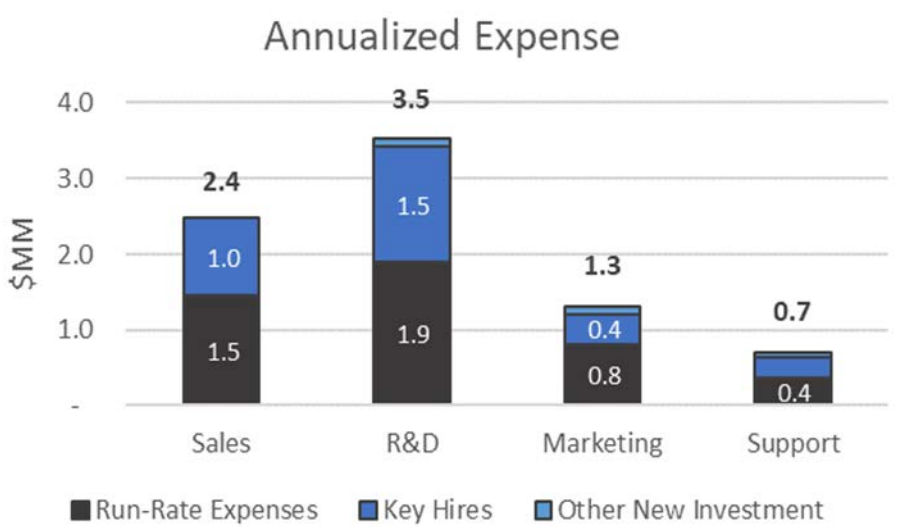
Select Balance Sheet Metrics

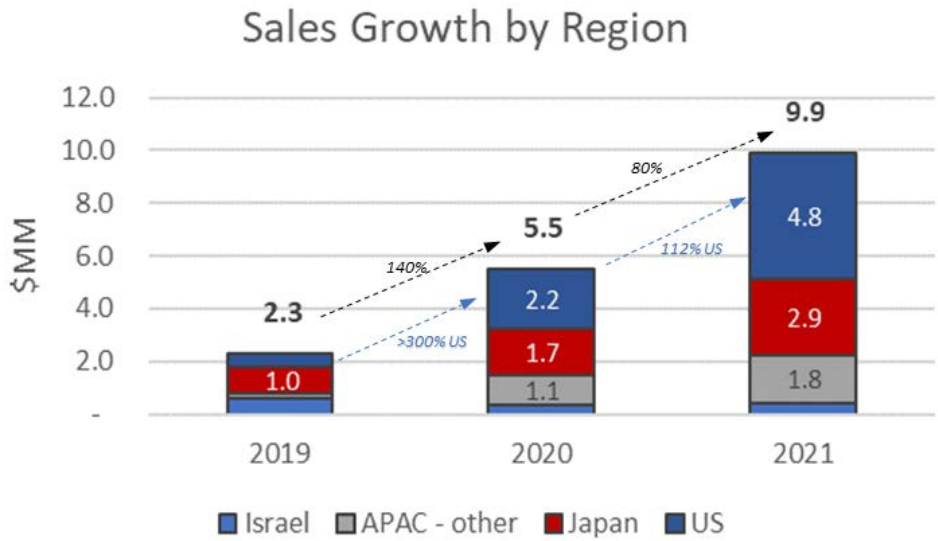
Deferred Revenues	2.2	2.6	5.1
Net Working Capital	(0.2)	0.0	0.0
Capital Assets	0.1	0.3	0.1

COMPANY FINANCIALS

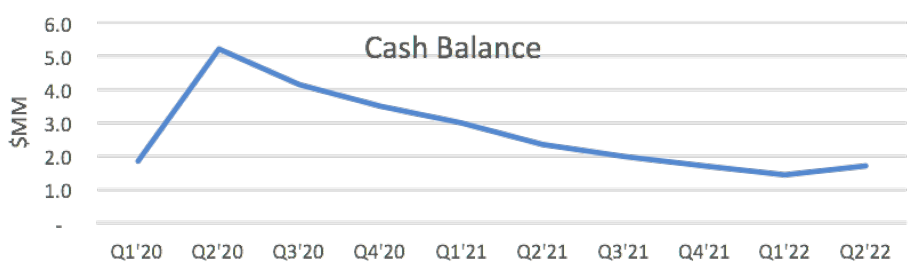
Use of Proceeds

- Series A funds the Votiro operating plan to positive cash-flow with $1.3M in cash reserve on the balance sheet at that point, February 2022
- Proceeds will be used to make key new operating investments to accelerate market fit and sales growth
- Use of proceeds from Series A to cash flow positive are summarized below for illustrative purposes



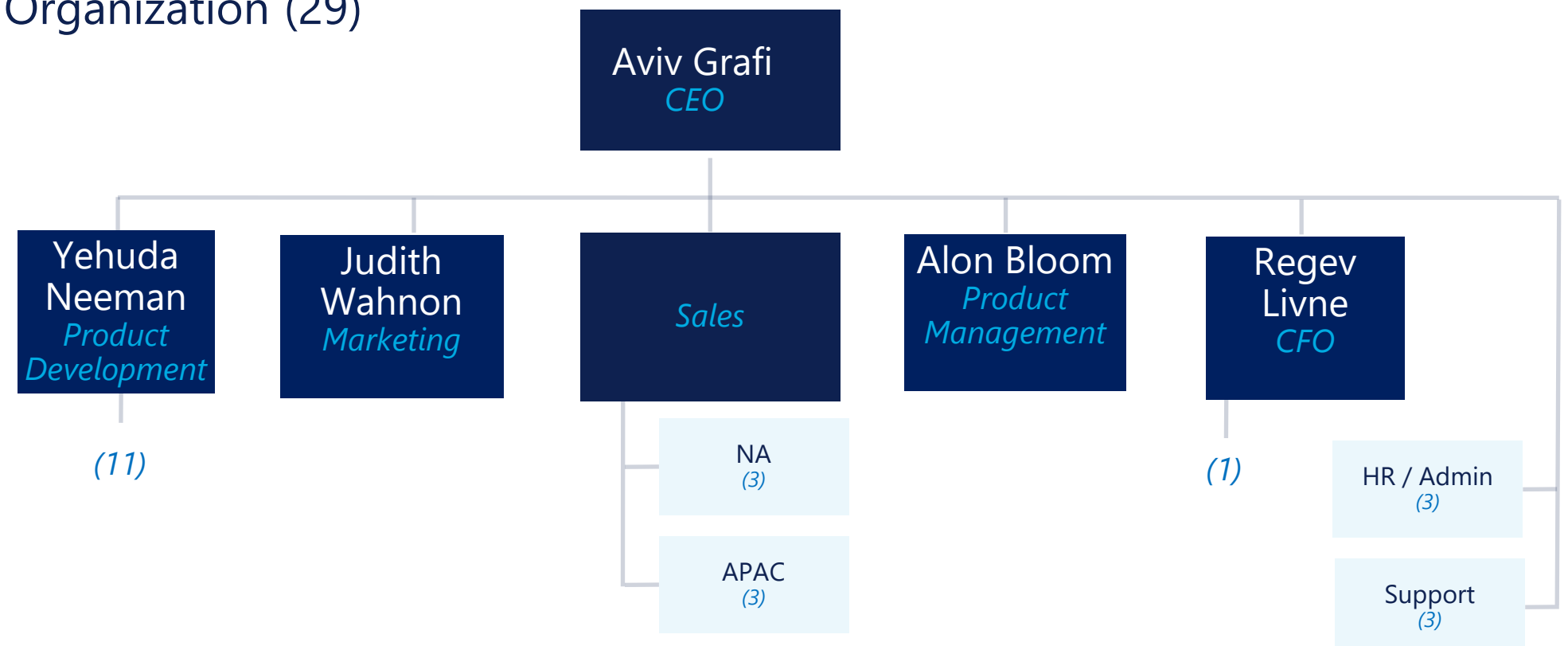


Annualized Recurring Revenue (ARR)		
2019	2020	2021
1.9	4.6	7.3



LEADERSHIP & STAFFING

Organization (29)



The next 20 months after Series A close headcount grows to 49

VOTIRO SECURED.

INVESTMENT HIGHLIGHTS

Market Timing & Cyber Security Trends	• 100% effective prevention of content-borne cyber attacks, incl. zero-days • Stops today's most virulent attacks, e.g. Ransomware
High Value, High ROI Solution to Blue Chip Customers	• Improves business productivity • Proven by sophisticated, demanding customers
Differentiated & Sustainable Technologies	• Patent protected intellectual property • A generation-plus ahead of CDR products • Robust and easy deployable Secure File Gateway
Streamlined, Experienced Management Team	• Industry leaders in global cyber security & intelligence community veterans
Leading Edge of the Company's Valuation Expansion	• Sales & product expansion from new investment • Continued strong US growth • Major blue-chip customer base
Attractive Investment in a Market-Leading Cyber Security Company	• The valuation of Votiro will increase dramatically over the next year

Thank You

Appendix of Reference Information

What is CDR?

Content Disarm and Reconstruction (CDR) is a cyber defense that protects against potentially malicious code hidden in content (files, documents, attachments, etc). Ideally the underlying CDR technologies remove malware by reconstructing the content using only components that are approved for the file type, ISO standard or company policy. By design, CDR should then not need to analyze or even detect the presence of malware, including exploits and weaponized content that have not been seen before. Reconstructed content should be known-safe regardless of the absence/presence or sophistication of any hidden attacks in the original. CDR is used to protect email, portals, website traffic, collaboration etc.

The success of first generation CDR was severely limited by the technology's continued reliance on finding, identifying and removing malware, plus, in some cases, the need to remove otherwise needed elements of the content.

What is Votiro?

Votiro was founded in Israel in 2012 by Aviv Grafi. The Company has raised a total of $14m in two separate capital raises. The second raise, in 2018, followed an extensive diligence to validate the technology and the business by Senetas Corp, which has to date invested $8m while implementing an expanded business model and appointing Aviv Grafi as the new CEO.

After introducing its first product in 2014, the Company experienced strong growth in 2015-2017 when it captured government mandated cyber security programs in Japan plus successes in Singapore. These wins in particularly demanding countries were strong validation of Votiro's next-gen CDR performance. The company's resources were getting stretched by the sudden APAC growth and it prevented expansion into other countries as fast as they wanted, specifically to the US.

When Senetas invested, they enabled entry to the US in 2019. Successes were quick and significant. In the second half of 2019 almost a $1m in subscriptions were booked by one sales person and one sales engineer in the US.