SPEAR

Cybersecurity Primer

Diving deep into opportunities in cybersecurity

February 2022

CONTENTS

EXECUTIVE SUMMARY:

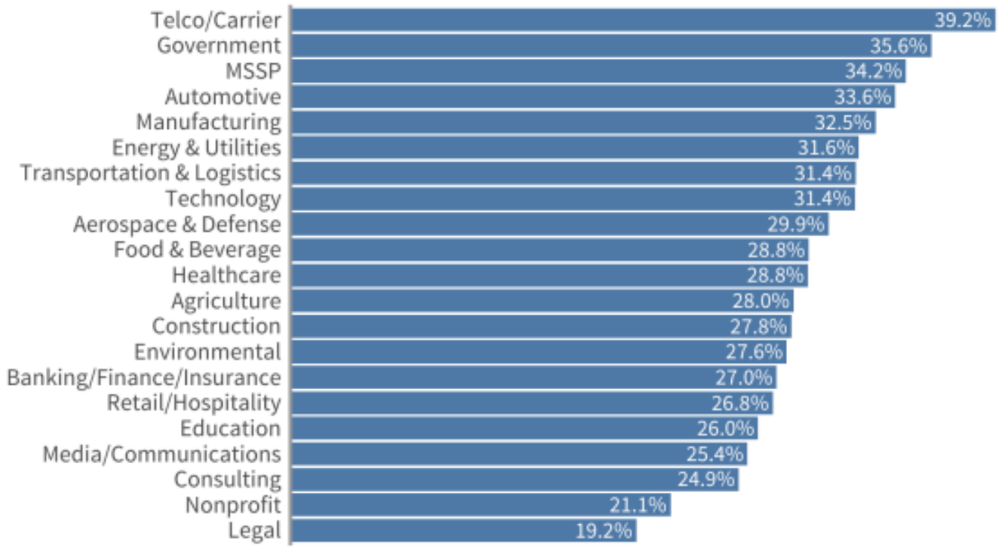
- The cybersecurity market is expected to grow at a double digit CARG with some areas growing 50%+, benefiting from increased number and complexity of cyberattacks and changes in data architecture
- Everchanging market requires constant development of new solutions to address new cyber threats, creating many investment opportunities
- We analyzed the different sub-segments and identified the following major trends:
  - Trend 1: **Cloud adoption creates need for "zero trust" solutions**– as organizations embrace digital transformation, legacy firewall providers are losing relevance creating opportunities for "zero trust" architectures
  - Trend 2: **Endpoint security needs "next-gen solutions"** – legacy solutions are inadequate and can only detect ~50% of threats. "Next-gen" predictive solutions based on artificial intelligence (AI) and machine learning (ML) are gaining market share and are expected to grow at a 20%+ CAGR for the next 5 years

Top picks: Zscaler (ZS), Palo Alto Networks (PANW)**, and **Microsoft (MSFT)

CONTENTS

Ransomware is affecting companies of all sizes and industries

Prevalence of ransomware detections across sectors in 1H21

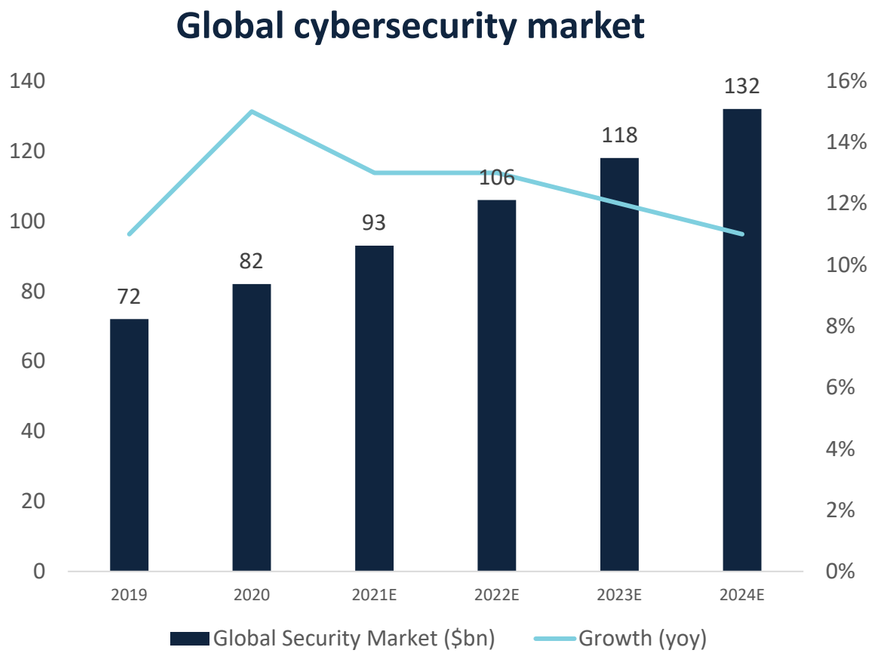


Source: Fortinet Global Threat Landscape Report, SPEAR Invest

- Contrary to general perceptions, ransomware presents a danger for a wider range of industries than just government, healthcare and education, according to a Fortinet report
- Examples of major attacks include Colonial Pipeline resulting in a severe disruption to fuel supplies, and JBS, similar disruption to meat supplies across the US
- Cybersecurity attacks are increasingly more complex vs. historically mostly consisting of phishing, malware (e.g., SolarWinds)

Ransomware attacks increasingly more complex as hackers are able to bypass legacy solutions

The global security market is expected to grow at low-teens CAGR



Source: Gartner, SPEAR Invest

Driver #1: increased number of attacks forcing companies to re-evaluate their cybersecurity policies

- The number of organizations impacted by ransomware globally **more than doubled in the first half of 2021 compared with 2020,** according to Checkpoint Research
- **Geopolitical tensions** can exacerbate cybersecurity threats
- Cybersecurity poses threats to companies of any size vs. previously attacks focused on larger organizations

Driver #2: Digital transformation and cloud migration introduce incremental cybersecurity risks

- **Workloads:** as companies continue to digitally transform by using public, hybrid, and multi-cloud environments, the traditional network perimeter has dissolved, introducing new security risks
- **Users:** as employees expand to multiple devices and locations (work-from-home etc.) the “attack surface” meaningfully increases
- Current firewall and VPN infrastructure can not adequately address new risks

Technology shifts driving 20%+ growth in select areas of cybersecurity

Market	**Network Security**	**Endpoint**	**Security management**	**Content**	**Cloud workloads**	**Other**	**Total**
Description	*Firewall/UTM, IDP, NAC*	*Corporate, Consumer, IoT*	*Identity, SIEM, Vulnerability*	*Web, Messaging, DLP*	*CNAPP, CSPM, CWPP*		
Market size ($bn)	~20	~16	~14	~8	<1	~30	~90
Market growth	8% Legacy/ **30%+ NGS**	**~20%**	**~15%**	~12%	**~40%+**		**~10% 5Y CAGR**
Key Players	Palo Alto Networks Fortinet Zscaler VMWare Check Point Cisco Juniper Symantec	Microsoft Crowdstrike SentinelOne VMWare Carbon Black McAfee Symantec (Broadcom)	Microsoft Authenticator Microsoft Sentinel Okta CyberArk PING Identity	Microsoft Symantec McAfee Cloudflair MIME Proofpoint	Palo Alto Networks Zscaler Cloudflair		

*Deffinitions**

NGS - Next Generation Solutions
UTM - Unified Threat Management
IDP - Intrusion Detection Prevention
NAC - Network Access Control

SIEM - Security Info Event Mgmt

DLP - Data Loss Prevention

CNAPP - Cloud-Native Application Protection Platform
CSPM - Cloud Security Posture Management
CWPP - Cloud Workload Protection Platform
CIEM - Cloud Infrastructure Entitlement Mgmt

Source: Gartner, IDC, SPEAR Invest

Constantly evolving threats create a need for innovative solutions, resulting in high growth segments and attractive investment opportunities

We focus on high growth end markets with secular growth drivers…

NETWORK SECURITY	ENDPOINT SECURITY	SECURITY MANAGEMENT	CLOUD
~$20bn **~10% CAGR**	**~$16bn** **~20% CAGR**	**~$14bn** **~15% CAGR**	**<$1bn** **~40-50% CAGR**
• Traditional firewalls and VPNs are in-adequate for todays environment with expanding network complexity (public and private cloud applications, multi-cloud environments) • Creating an opportunity for new entrants with innovative simple architectures to gain significant market share	• Traditional endpoint protection (e.g. antivirus) only detects a portion of threats • Endpoint has increased in importance as networks have become distributed with increasing number of access points (phones, mobile devices, laptops) • Opportunity for new solutions based on AI and ML to gain share	• Identity Access Management (IAM) and Privileged Access Management (PAM) are the largest markets, which enable the authentication of users and privileged accounts and subsequently provide access and controls • Digital transformation is a key driver of demand along with “next gen” security architectures	• Protecting workloads within the cloud and across different clouds is a new high growth market • Innovative architectures that are gaining share in network security can expand their applications to protect workloads in the cloud

Source: Gartner, IDC, SPEAR Invest;

…and strong innovative players

NETWORK SECURITY	ENDPOINT SECURITY	SECURITY MANAGEMENT	CLOUD
~$20bn ~10% CAGR	~$16bn ~20% CAGR	~$14bn ~15% CAGR	<$1bn ~40-50% CAGR
paloalto NETWORKS FORTINET zscaler CLOUDFLARE	Microsoft CROWDSTRIKE SentinelOne vmware Carbon Black.	Microsoft okta CYBERARK	zscaler paloalto NETWORKS CLOUDFLARE

Source: Gartner, IDC, SPEAR Invest

CONTENTS

Trend #1: Traditional firewall security is inadequate for the current network architecture

Network Security

Traditional WAN

- In traditional WAN architecture, traffic from branch locations is backhauled to corporate data centers
- This occurs via a multi-protocol label switching (MPLS) network - a private network provided by carriers and telcos
- Virtual Private Network (VPN) is used for users who reside outside the network

Drawbacks

- MPLS is expensive, offers low bandwidth and performance, time consuming and difficult to scale

Software Defined (SD-WAN)

- Virtualized network – brings intelligence that existed in hardware to into programable software
- SD-WAN relies on traditional broadband internet connection, although traffic can still be backhauled to the branch (significantly cheaper, as much as ~10x than MPLS)
- SD-WAN can intelligently route traffic connecting branches with data centers for on-premise apps, while bypassing the corporate network for cloud-based apps

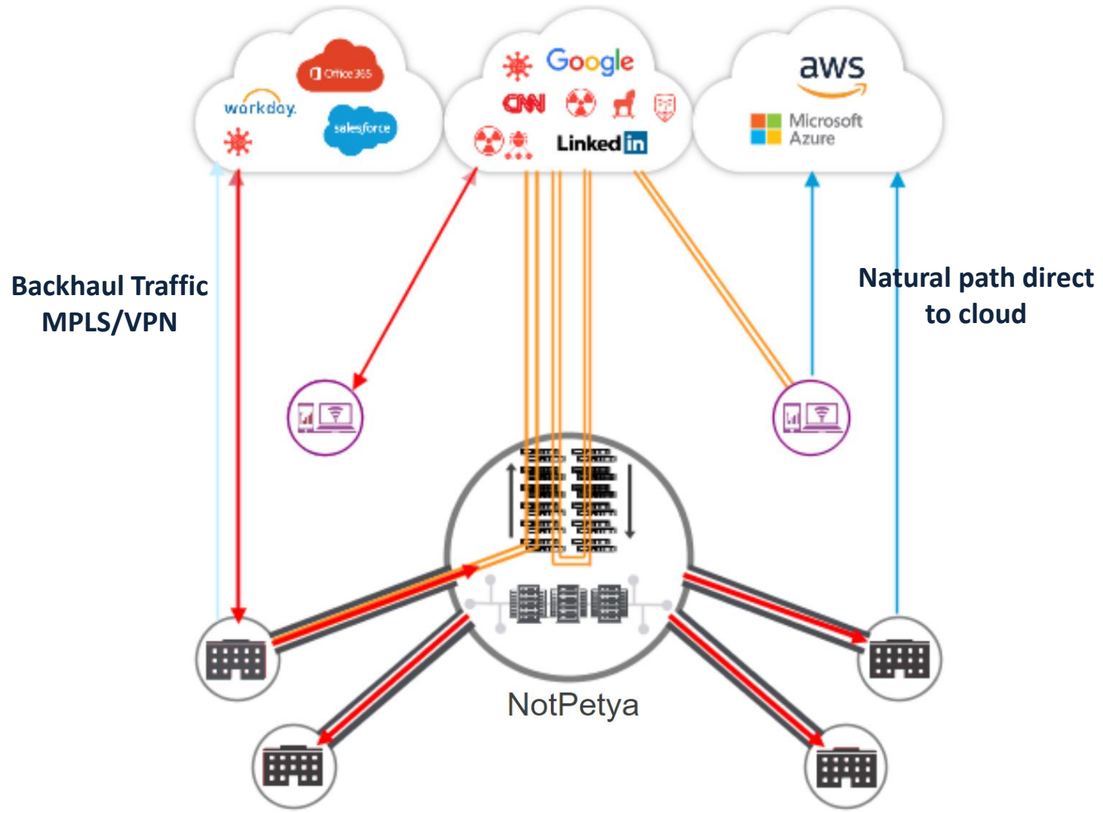
Optimal Set-up

- **SD-WAN** that connects to **proxy-based architecture** that stands between the users and the internet or the cloud

Proxy based architectures are gaining share from legacy firewalls and are growing at 30%+ CAGR, significantly higher than the overall market

The cloud is breaking legacy networks and security

The Cloud is the NEW Data Center



But security is still sitting in the OLD Data Center

Source: Zscaler

Downsides of legacy infrastructure:

- Poor user experience with increased latency
- High MPLS backhaul costs
- Significantly higher security risk
  - Increased attack surface
  - Risk of lateral threat movement
  - Passthrough firewall architecture has limited ability to inspect

Upsides of cloud-based architecture:

- High security – every instance needs to go through and be cleared by a proxy
- Cost efficient – companies can reduce hardware and MPLS costs by as much at 70%*
- Improved user experience – fast secure connection for users and workloads

* Siemens reported ~70% MPLS and hardware cost reduction by deploying Zscaler

Trend #2: Traditional end-point protection is ineffective, creating the need for **“next gen”** end-point detection and protection (EDP) solutions

Endpoint detection and protection (EDP) market shares

	2019	2020	Market share direction	
CrowdStrike	8%	12%	↑	**Next-gen EDP 30% CAGR**
Microsoft	6%	10%	↑	
SentinelOne	1%	2%	↑	
Vmware Carbon Black	5%	5%	↔	
Trend Micro	9%	8%	↓	**Traditional EPP ~10%+ CAGR**
Broadcom Symantec	10%	6%	↓	
McAfee	10%	8%	↓	
Other	51%	49%	↓	
Total	100%	100%		**Total EPP market ~20% CAGR**

Source: IDC, Spear Invest

- Endpoint is a valuable security entry point as highlighted by recent ransomware breaches (e.g. Colonial Pipeline, JBS)
- Traditional endpoint protection products (EPP) **e.g. antivirus** scans are now only effective in blocking basic malware, not the type of attacks companies are experiencing today
- Prevention based “next-gen” tools (NGAV) provide **visibility, threat context** and **remediation capabilities**
- Microsoft, Crowdstrike and SentinelOne have been gaining significant market share at the expense of traditional players (Mcafee and Symantec)

“Next-gen” solution based on AI and ML are gaining significant share growing at >30% CAGR

Next-gen EDP players that will benefit from 30%+ end market growth

Microsoft

- **Leading endpoint provider** (Microsoft Defender) – impressive market share gains ~400bp 20vs.19;
- ~600mm EDP business growing at 90%+ rate (20/19)
- Endpoint products are built into Windows and Azure – most share gain in lower-end markets looking to consolidate vendors
- Combines identity security, cloud app security, and endpoint protection

CROWDSTRIKE

- **Leader** in accounts with >500 employees (60% of EDM TAM)
- Products are priced at a premium to Microsoft and SentinelOne (as much as ~40%); targeting higher-end market
- Revenue base of ~900mm, growing at 80% in '21 and trading at 16x '23E revenue
- Technology differentiation: security processing is performed on the cloud
- Concern is high multiple and increased competition, but it is a large and growing market

SentinelOne

- **Very strong** in the SMB/mid-market (40% of EDM TAM)
- Good fit for smaller price-conscious customers
- Revenue base of ~100mm, growing at 100%+ and trading at 17x '23E revenues
- Technology differentiation: security processing is performed locally at the end-point using ML based malware prevention

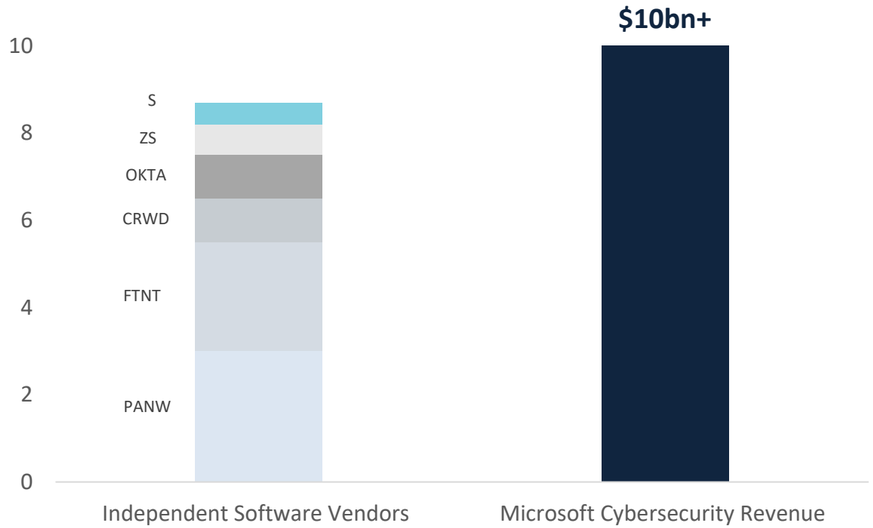
Carbon Black. / vmware

- End-to-end security infrastructure across endpoint, networking, and workloads. Similar to Microsoft, VMW is looking to leverage existing installed base. Cybersecurity is ~$1bn in revenue/ Carbon Black ~$300mm
- Carbon Black is increasingly picking up customer interest. VMWare acquired the company in 2019 for $2.1bn
- VMWare is inexpensive - trading ~15x FCF; cybersecurity opportunity may be underappreciated

CONTENTS

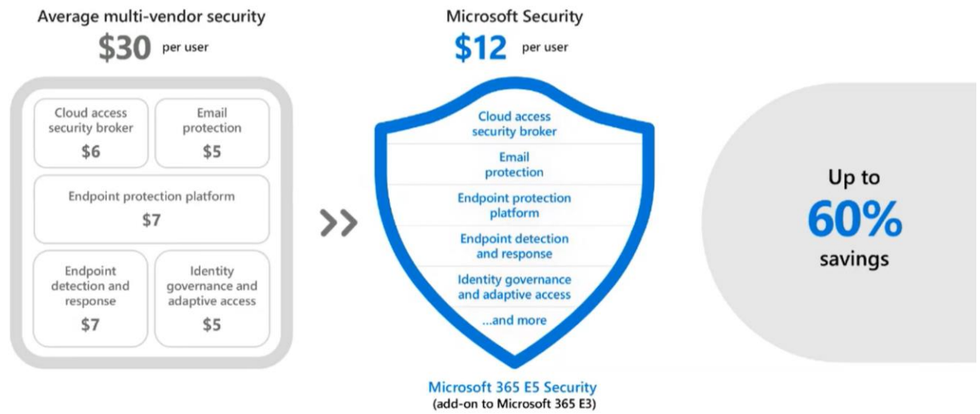
Case study #1: Microsoft is becoming a cybersecurity leader with 40%+ growth on a large revenue base

Microsoft cybersecurity business exceed the industry's largest players combined revenues



Source: Company reports, Spear Invest; MSFT LTM revenue ~$10bn as of Jan, 2021 (40% growth yoy)

Microsoft offers a price competitive package – up to 60% savings



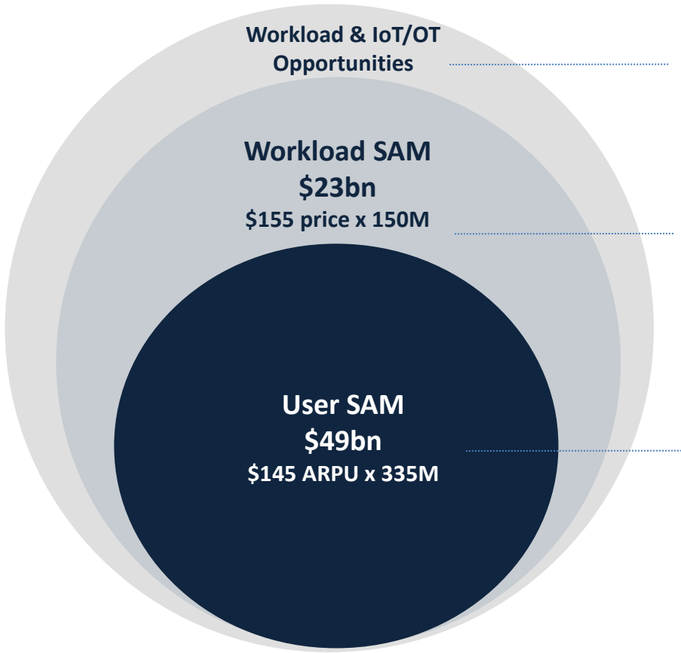
Leader in identity security, cloud app security, and endpoint protection

*Cybersecurity can add **200bp incremental growth** to Microsoft total revenue (on top of a healthy ~15% historical 5-year growth CAGR)*

Case study #2: Zscaler – a differentiated platform built for the cloud

- Differentiated “Zero Trust Exchange” securely connects each user to applications in the cloud
- Massive scale processes 200+billion daily transactions; 7bn daily enforcements
- Products significantly reduce complexity and cost while increasing security
- Large addressable market allows the company to grow at a **30%+ rate for 10+ years** from todays revenue base of ~**$1bn**

Zscaler addressable markets for users and workloads



Source: Company reports, Spear Invest;

Underappreciated ability to maintain 30%+ growth for over 10 years driven by large growing addressable market, potential for upselling to existing users, and introduction of new products

Case study #3: Palo Alto Networks legacy platform undergoing a transformation

Palo Alto Networks Platform		
Network Security	**Cloud**	**Security automation**
Strata (Firewall) Prisma SASE	**Prisma Cloud**	**Cortex**
• SD-WAN to become largest segment by 2025; rapid SASE adoption +68% yoy • >25% of Prisma SASE customers are new to PANW	• Prisma cloud customers +30% yoy; • credits consumed +70% yoy • Cloud security TAM ~$20bn • $300mm in ARR	• TAM of $45bn by 2024 (includes endpoint) • Products growing 60-100%+ although from small base

- Palo Alto is in the process of transforming itself from a legacy firewall vendor to a security platform company (next-gen products include cloud, endpoint, and AI)
- Platform approach could be beneficial as Palo Alto leverages “next-gen” solutions to its existing 80K+ costumer base
- “Next –gen” products represented ~25% of billings in F1Q21 showing meaningful traction
- Legacy firewall products provide a strong foundation of existing customer base which we believe is underappreciated by the market

Palo Alto Networks can leverage its existing customer base to continue to grow its recently assembled portfolio of “next gen” assets at 50%+ growth rates

DISCLOSURES:

The content of this presentation is **for informational purposes only** and is subject to change without notice.

This presentation does not constitute, either explicitly or implicitly, **any provision of services or products by SPEAR** and investors are encouraged to consult counsel and/or other investment professionals as to whether a particular investment management service is suitable for their investment needs.

All statements made regarding companies or securities are strictly beliefs and points of view held by **SPEAR** and are NOT endorsements by **SPEAR** of any company, or security or recommendations by **SPEAR** to buy, sell or hold any security.

Historical results are not indications of future results. Certain of the statements contained in this presentation may be statements of future expectations and other forward-looking statements that are based on **SPEAR**'s current views and assumptions and involve known and unknown risks and uncertainties that could cause actual results, performance or events to differ materially from those expressed or implied in such statements.

The matters discussed in this presentation may also involve risks and uncertainties described from time to time in **SPEAR**'s filings with the U.S. Securities and Exchange Commission. **SPEAR** assumes no obligation to update any forward-looking information contained in this presentation.

Certain information was obtained from sources that **SPEAR** believes to be reliable; however, **SPEAR** does not guarantee the accuracy

or completeness of any information obtained from any third party.

SPEAR and its clients as well as its related persons may (but do not necessarily) have financial interests in themes, securities, or issuers that are discussed.