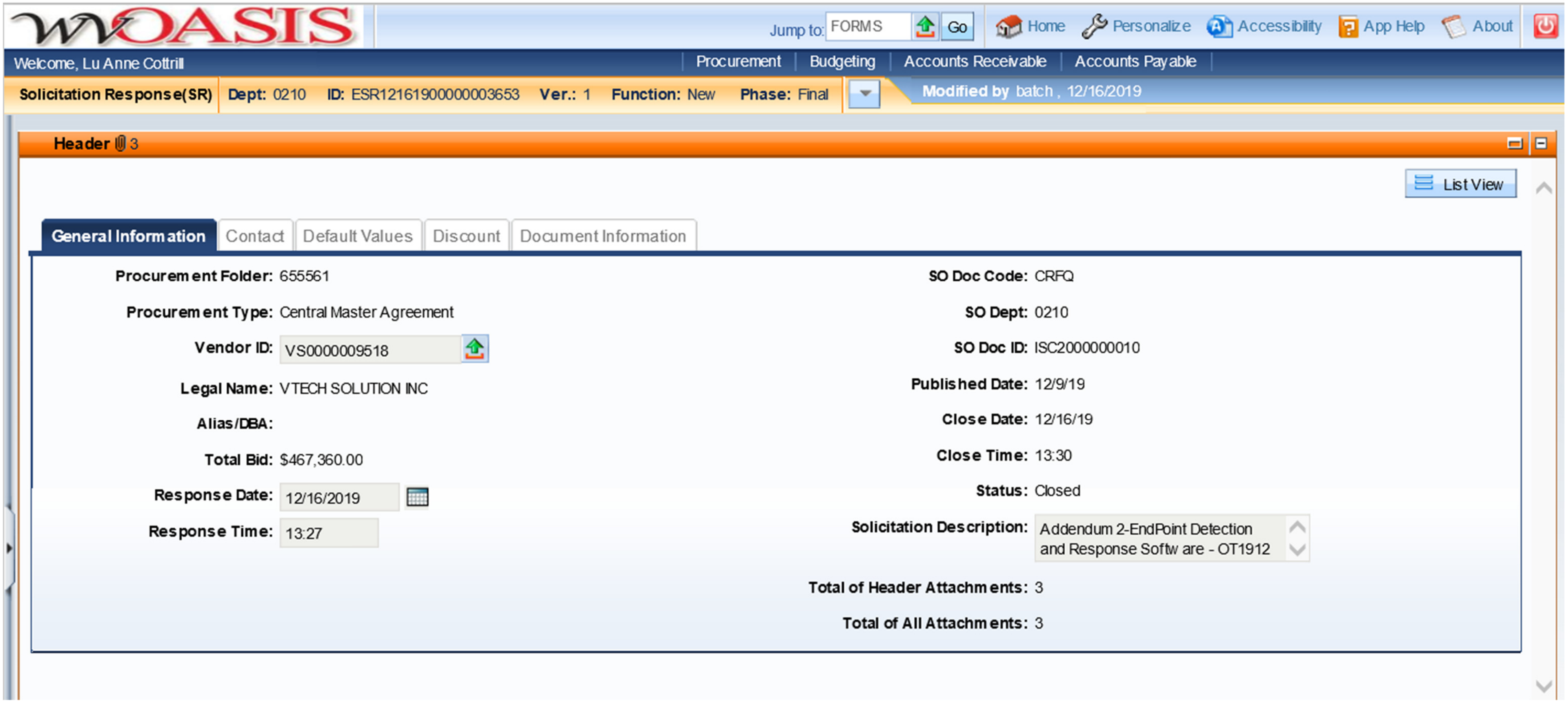
West Virginia
Purchasing Division

2019 Washington Street, East
Charleston, WV 25305
Telephone: 304-558-2306
General Fax: 304-558-6026
Bid Fax: 304-558-3970

The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at *wvOASIS.gov*. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at *WVPurchasing.gov* with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.



Welcome, Lu Anne Cottrill

Solicitation Response(SR) Dept: 0210 ID: ESR1216190000000003653 Ver.: 1 Function: New Phase: Final

Modified by batch , 12/16/2019

Header 3

Procurement Folder:	655561	SO Doc Code:	CRFQ
Procurement Type:	Central Master Agreement	SO Dept:	0210
Vendor ID:	VS0000009518	SO Doc ID:	ISC2000000010
Legal Name:	VTECH SOLUTION INC	Published Date:	12/9/19
Alias/DBA:		Close Date:	12/16/19
Total Bid:	$467,360.00	Close Time:	13:30
Response Date:	12/16/2019	Status:	Closed
Response Time:	13:27	Solicitation Description:	Addendum 2-EndPoint Detection and Response Softw are - OT1912
		Total of Header Attachments:	3
		Total of All Attachments:	3

Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Solicitation Response

Proc Folder : 655561

Solicitation Description : Addendum 2-EndPoint Detection and Response Software - OT1912

Proc Type : Central Master Agreement

Date issued	Solicitation Closes	Solicitation Response	Version
	2019-12-16 13:30:00	SR 0210 ESR12161900000003653	1

VENDOR

VS0000009518

VTECH SOLUTION INC

Solicitation Number: CRFQ 0210 ISC2000000010

Total Bid : $467,360.00 **Response Date:** 2019-12-16 **Response Time:** 13:27:40

Comments: Already provided discounted quotations.

FOR INFORMATION CONTACT THE BUYER

Jessica S Chambers
(304) 558-0246
jessica.s.chambers@wv.gov

Signature on File **FEIN #** **DATE**

All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	CNTRCT ITEM: Containment Remediation Reporting & Monitoring	2000.00000	EA	$52.340000	$104,680.00

Comm Code	Manufacturer	Specification	Model #
43233204			

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Opt Renew Y2 - Cntrct Item: Contain Remediate Report Monitor	2000.00000	EA	$57.340000	$114,680.00

Comm Code	Manufacturer	Specification	Model #
43233204			

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	Opt Renew Y3 - Cntrct Item: Contain Remediate Report Monitor	2000.00000	EA	$62.000000	$124,000.00

Comm Code	Manufacturer	Specification	Model #
43233204			

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	Opt Renew Y4 - Cntrct Item: Contain Remediate Report Monitor	2000.00000	EA	$62.000000	$124,000.00

Comm Code	Manufacturer	Specification	Model #
43233204			

Extended Description :

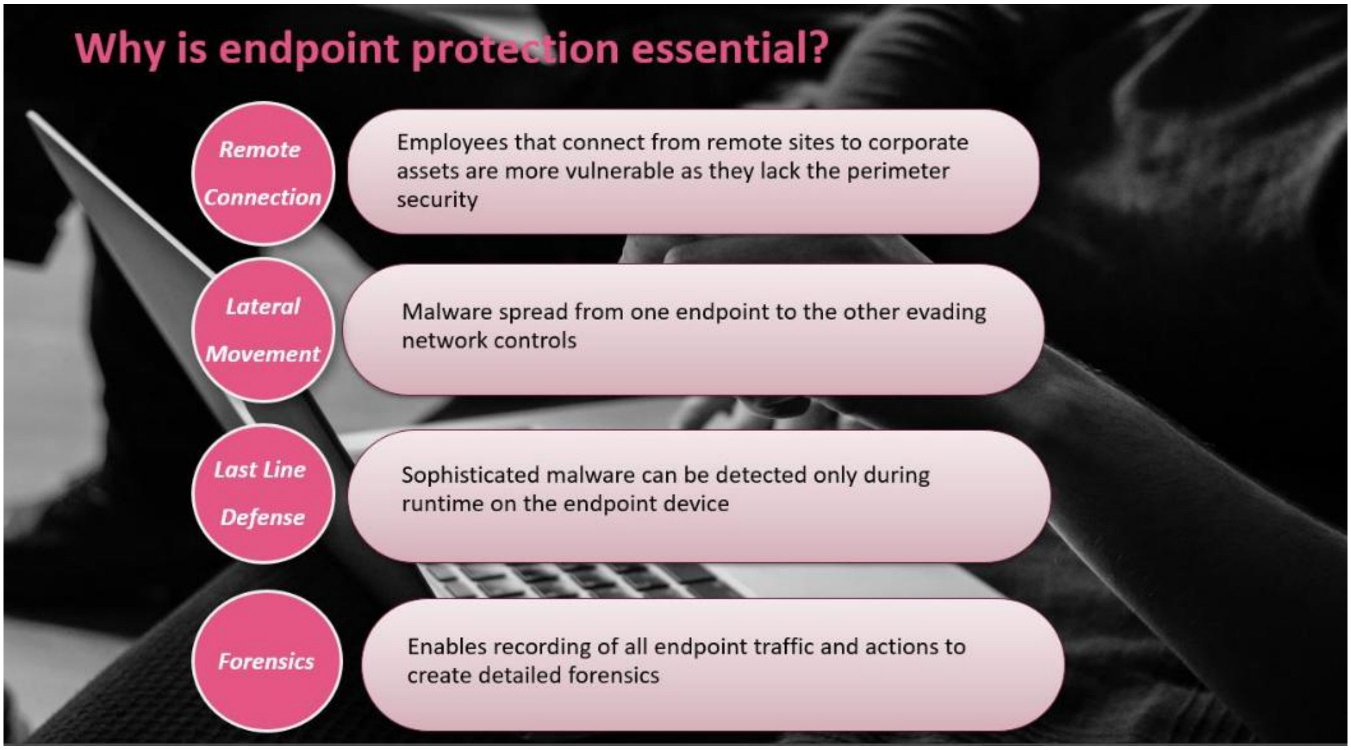
4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

TECHNICAL SOLUTION

We are proposing our solution for this requirement is Checkpoint Completed protection – Sandblast endpoint agent. Below is knowledge sharing with State of West Virginia about this solution

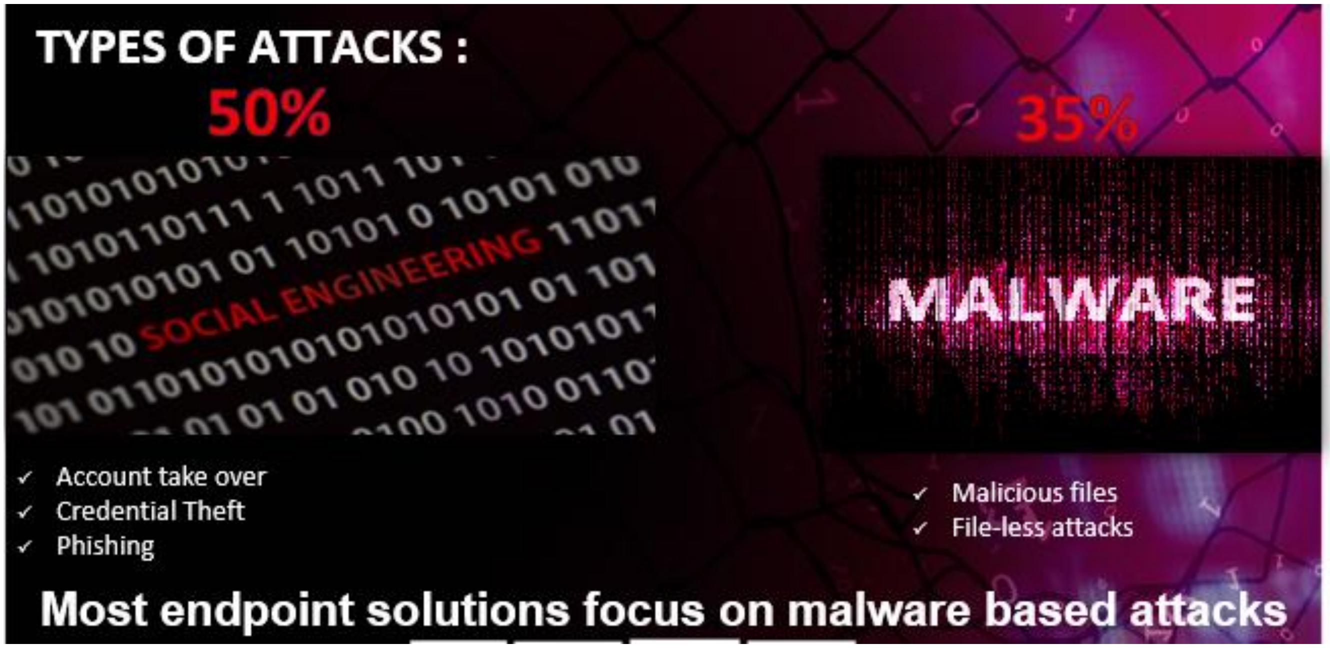
WHY NEED EDR



Why is endpoint protection essential?

- **Remote Connection**: Employees that connect from remote sites to corporate assets are more vulnerable as they lack the perimeter security
- **Lateral Movement**: Malware spread from one endpoint to the other evading network controls
- **Last Line Defense**: Sophisticated malware can be detected only during runtime on the endpoint device
- **Forensics**: Enables recording of all endpoint traffic and actions to create detailed forensics

WHERE DO WE MISS THREATS?



TYPES OF ATTACKS :

50%

- ✓ Account take over
- ✓ Credential Theft
- ✓ Phishing

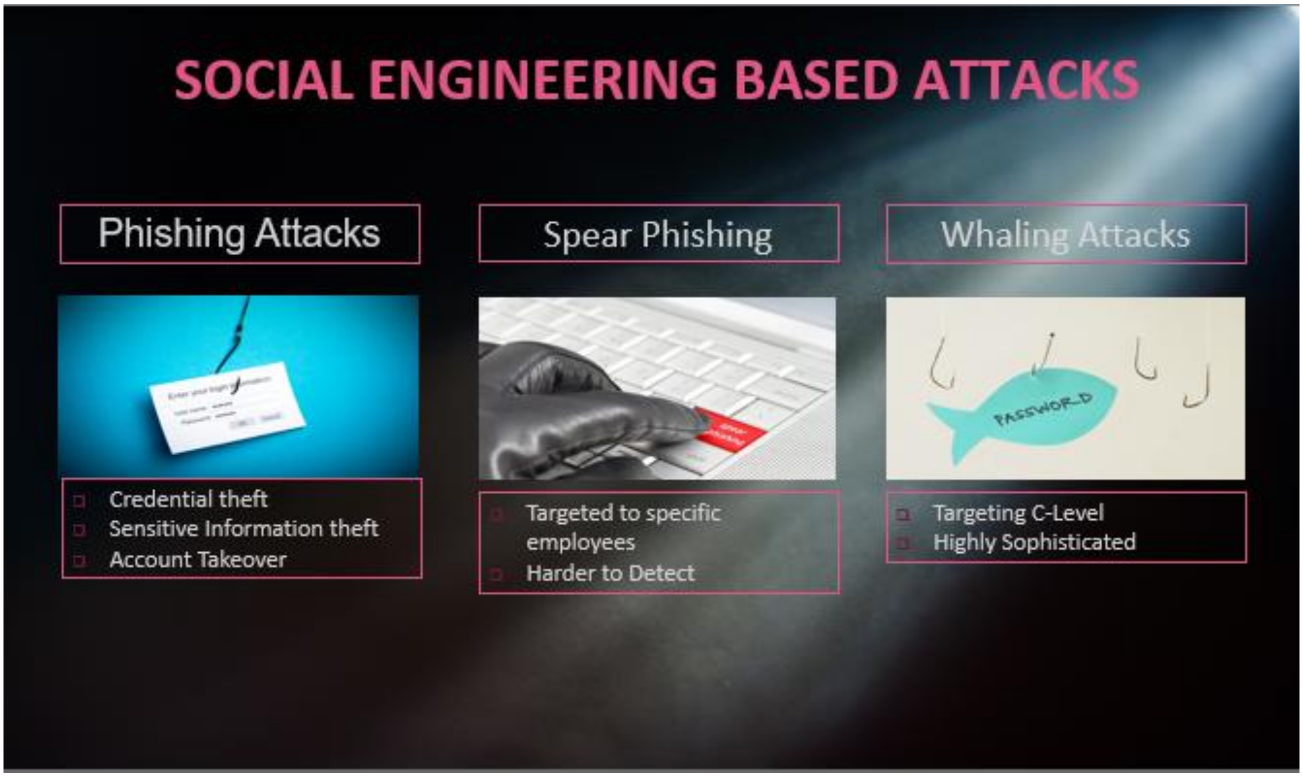
35%

- ✓ Malicious files
- ✓ File-less attacks

Most endpoint solutions focus on malware based attacks

So when it comes to attacks that will target employees and devices, we can divide them into two:

- The 1st one involves social engineering, these attacks represent the vast majority of the threats (little bit over 50% of such attacks) involve social engineering, which means that no malicious file is going to be involved.
- Attacker will invest in mimiking a legitimate web site or will send a legit e-mail with a link to a phishing website, which mimiks a legit web site, waiting for the user to use his credential in attempt to steal it, as account takeover attack (credential theft) through phishing attack.
- Attackers may be interested in stealing also credentials of personal application in order to use it later, to attack the corporate assets. So according to our findings 50% of the attacks will not involve any malicious malware and will try to steal the user accounts either for personal or corporate applications.
- While looking at the remaining attacks, 35% of them, they involve a download of a malicious malware, primarily via a downloaded file, in order to get execution privileges on the infected devices to create damage, that will usually come in the form of a zero-day attack and once infected the malware will try to create more damage, usually via lateral movement, it will try identify more servers in which it can steal information from.
- It's important to note that today most if not all EP players will NOT offer a good protection against zero-day social engineering.
- The URL Fileting and the AntiSpam will protect only against the known phishing and social engineering attacks. They focus only on the malware, the ability to detect known and unknown malware and malicious files.



SOCIAL ENGINEERING BASED ATTACKS

Phishing Attacks

- Credential theft
- Sensitive Information theft
- Account Takeover

Spear Phishing

- Targeted to specific employees
- Harder to Detect

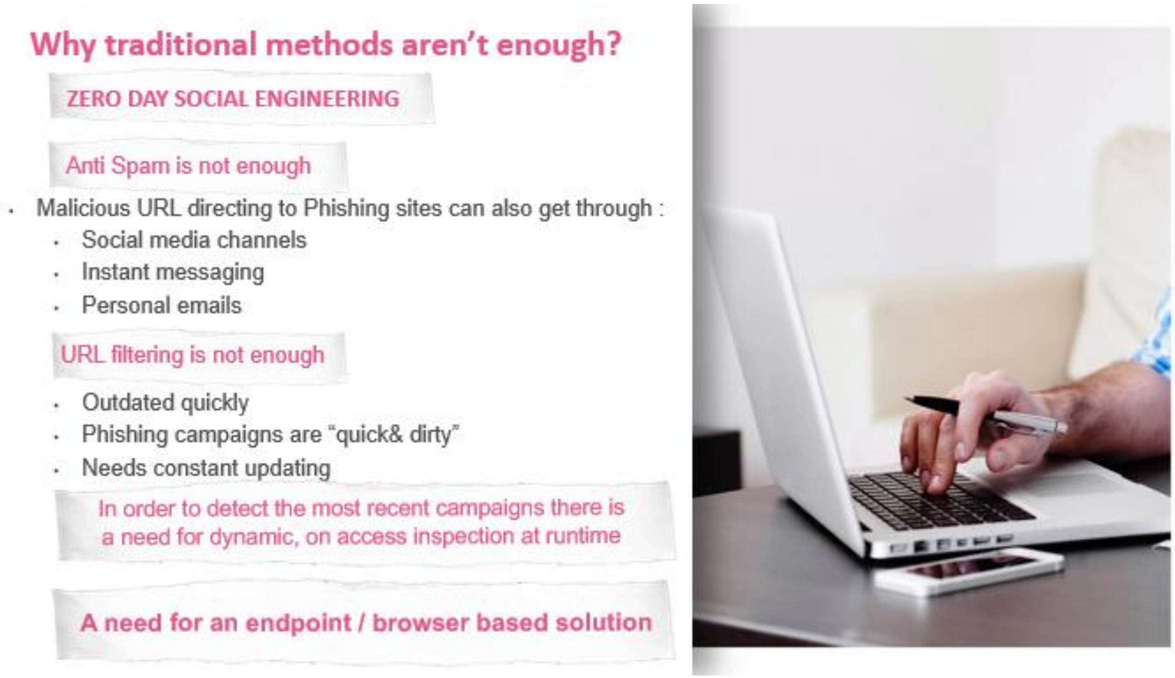
Whaling Attacks

- Targeting C-Level
- Highly Sophisticated

These attacks usually start with a very generic phishing mail, this is where the attacker will send a batch of million spam messages to many consumers and employees with the hope that some of them will surrender their credentials, either corporate credential, banking applications, social media applications or other, those could be used later to hack into the corporate perimeter.

We also see spear phishing attacks; these are the attacks that try to target specific individuals or specific organizations.

We are also seeing over the last few years a growth is what it called whaling attacks, those are the attacks which try to steel the e-mail accounts or credentials of the CEO, in order to send e-mail from his account to the CFO, asking him to wire funds to a new supplier of the organization.



Why traditional methods aren't enough?

ZERO DAY SOCIAL ENGINEERING

Anti Spam is not enough

- Malicious URL directing to Phishing sites can also get through :
  - Social media channels
  - Instant messaging
  - Personal emails

URL filtering is not enough

- Outdated quickly
- Phishing campaigns are "quick& dirty"
- Needs constant updating

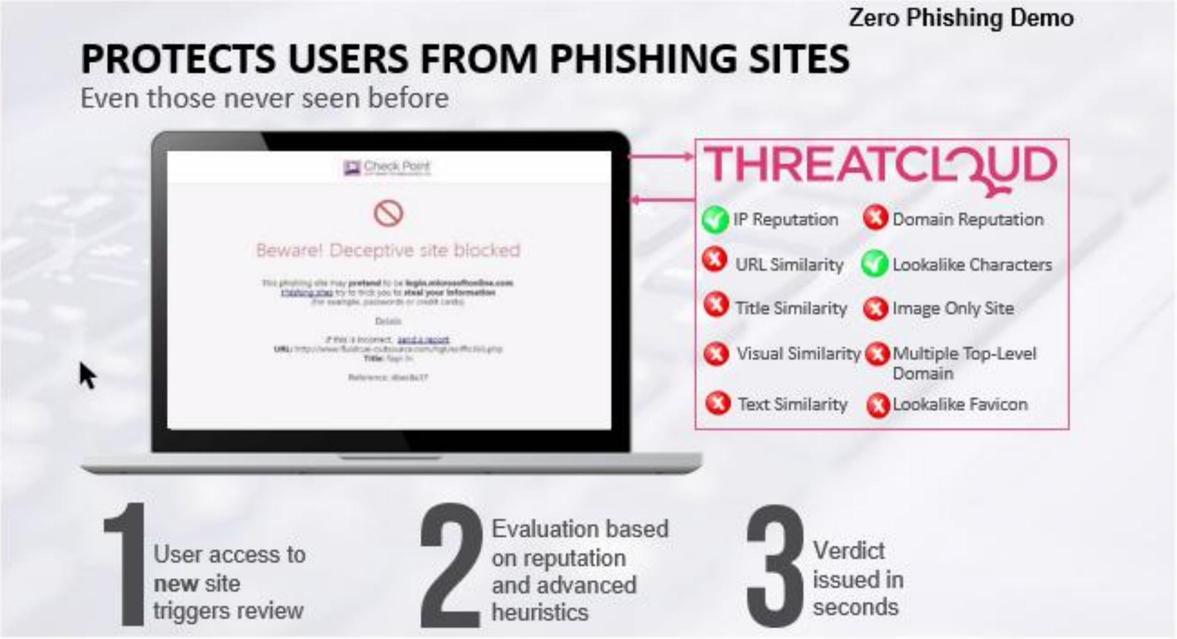
In order to detect the most recent campaigns there is a need for dynamic, on access inspection at runtime

A need for an endpoint / browser based solution

Traditional solutions against social engineering attacks are not going to be sufficient. They deal with knows social engineering attacks but will know do not deal with zero-day social engineering and account take over attacks.

The 1st and the main solution that most organizations are going to use is Anti-Spam, however antispam can be easily bypassed, since the links to the phishing web site, could be shared via other means of media, such as social media channels, instant messaging (like Facebook and LinkedIn) or through personal public e-mail like g-mail, which are not protected by a strong Anti-Spam solutions.

When it comes to URL filtering, this solution handles only known URLs, however attackers are going to act very quickly and change the URL to a new uncategorized URL and unless the URL Filtering blocks access to uncategorized web sites, such access won't be prevented. In such case, the organization is likely to suffer from high rate of false positives and for that reason, there is a need to deploy a solution that will analyze dynamically the website itself, during runtime on the browser in order to identify dynamically zero-day phishing web sites.



Zero Phishing Demo

PROTECTS USERS FROM PHISHING SITES

Even those never seen before

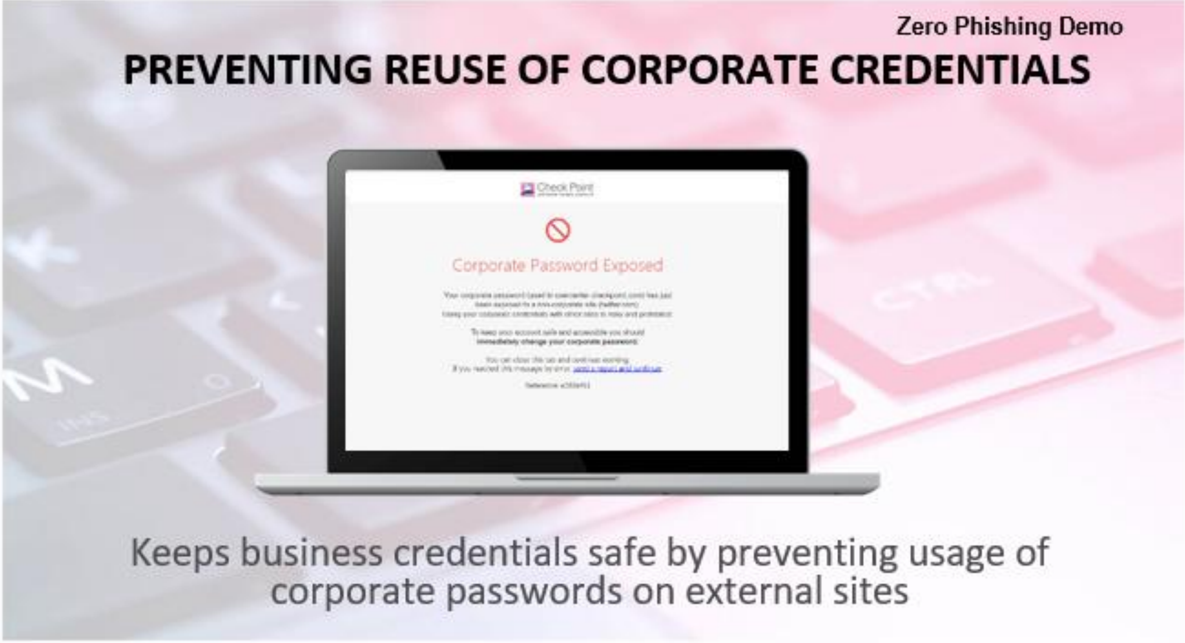
THREATCLOUD

✓ IP Reputation	✗ Domain Reputation
✗ URL Similarity	✓ Lookalike Characters
✗ Title Similarity	✗ Image Only Site
✗ Visual Similarity	✗ Multiple Top-Level Domain
✗ Text Similarity	✗ Lookalike Favicon

1 User access to **new** site triggers review

2 Evaluation based on reputation and advanced heuristics

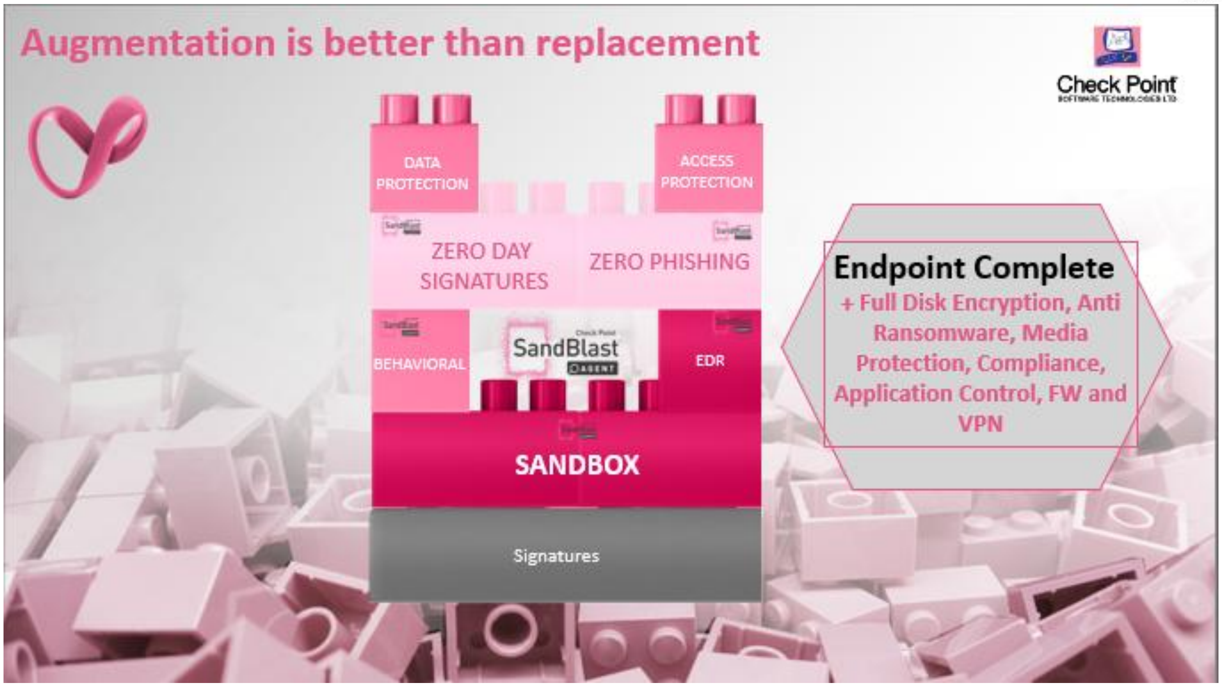
3 Verdict issued in seconds



Zero Phishing Demo

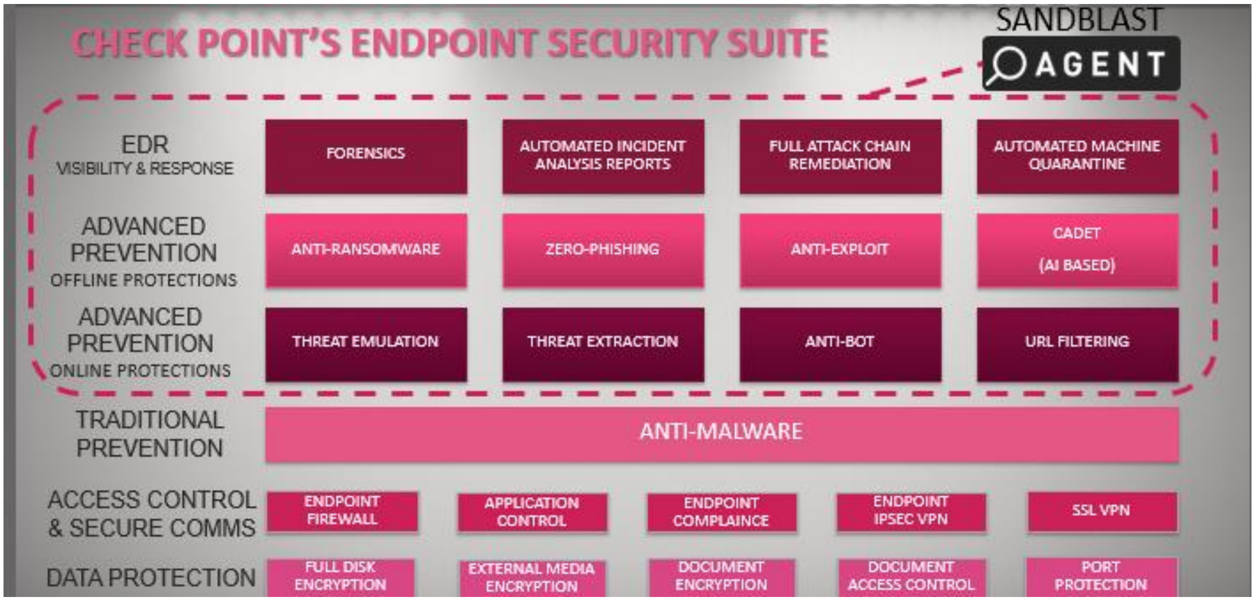
PREVENTING REUSE OF CORPORATE CREDENTIALS

Keeps business credentials safe by preventing usage of corporate passwords on external sites



Augmentation is better than replacement

Endpoint Complete
+ Full Disk Encryption, Anti Ransomware, Media Protection, Compliance, Application Control, FW and VPN



CHECK POINT'S ENDPOINT SECURITY SUITE

SANDBLAST AGENT

EDR VISIBILITY & RESPONSE	FORENSICS	AUTOMATED INCIDENT ANALYSIS REPORTS	FULL ATTACK CHAIN REMEDIATION	AUTOMATED MACHINE QUARANTINE	
ADVANCED PREVENTION OFFLINE PROTECTIONS	ANTI-RANSOMWARE	ZERO-PHISHING	ANTI-EXPLOIT	CADET (AI BASED)	
ADVANCED PREVENTION ONLINE PROTECTIONS	THREAT EMULATION	THREAT EXTRACTION	ANTI-BOT	URL FILTERING	
TRADITIONAL PREVENTION	ANTI-MALWARE				
ACCESS CONTROL & SECURE COMMS	ENDPOINT FIREWALL	APPLICATION CONTROL	ENDPOINT COMPLAINCE	ENDPOINT IPSEC VPN	SSL VPN
DATA PROTECTION	FULL DISK ENCRYPTION	EXTERNAL MEDIA ENCRYPTION	DOCUMENT ENCRYPTION	DOCUMENT ACCESS CONTROL	PORT PROTECTION

Qualification Points In Terms of Requirements Requested By State Of West Virginia –

We believe this EDR solution proposed by vTech is complete match with the requirement if State of West Virginia.

However, to ensure before purchase if State of West Virginia requires product demo or Proof of Concept for the proposed product, we will be able to arrange free of cost.

NOTE:

Please find the below mentioned point to review regarding capabilities of solution.

4.1.2.1 From list of requirements the only mismatch we found that our proposed solution in not supported on Linux platform. However, client servers using VMware, Azure or Hyper- V running on Windows OS are supported by this solution.

(4.1.1.3.9-) We are not sure what will be exact definition of an Isolation container is however if this refers to Quarantined files as you state our software does continue to monitor after the quarantine process.

(4.1.1.3.23) – Software should be able to automatically discover and alert on previously known external/internal hardware connected to endpoints for purpose of retrospective/post event analysis: -
This is not included in the forensics blade however the Media Encryption & Port Protection component protects sensitive information by encrypting data and requiring authorization for access to storage devices, removable media and other input/output devices. Administrators use the Smart Endpoint to create rules for data encryption, authorization and access to devices. These rules are part of the Endpoint Security policy installed on endpoint computers.

PRICING TABLE

QTY	MFR #	DESCRIPTION	PRICE EA.	EXTENDED
2000	CPEP-SBA-COMPLETE-1Y	S&BLAST AGENT COMPLETE 1YR PROVIDES ADV, SUPPORT INCLUDED (REMOTE AND ON- SITE)	$ 52.34	$ 104,680.00
1	PROFESSIONAL SERVICES (OPTIONAL)	OPTIONAL INITIAL CONFIGURATION, INSTALLATION AND SETUP SERVICES	$ 15,000.00	$ 15,000.00
			Total	**$ 119,690.00**

ADDENDUM ACKNOWLEDGEMENT FORM

SOLICITATION NO.: CRFQ 0210 ISC2000000010

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[✓] Addendum No. 1

[ ] Addendum No. 2

[ ] Addendum No. 3

[ ] Addendum No. 4

[ ] Addendum No. 5

[ ] Addendum No. 6

[ ] Addendum No. 7

[ ] Addendum No. 8

[ ] Addendum No. 9

[ ] Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

vTech Solution Inc.
Company

Authorized Signature

12/16/2019
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: ____________

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[ ] Addendum No. 1

[✓] Addendum No. 2

[ ] Addendum No. 3

[ ] Addendum No. 4

[ ] Addendum No. 5

[ ] Addendum No. 6

[ ] Addendum No. 7

[ ] Addendum No. 8

[ ] Addendum No. 9

[ ] Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

vTech Solutioon Inc
Company

Authorized Signature

12/16/2019
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

Purchasing Divison
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Request for Quotation
21 — Info Technology

Proc Folder: 655561

Doc Description: Addendum 2-EndPoint Detection and Response Software - OT1912

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2019-12-09	2019-12-16 13:30:00	CRFQ 0210 ISC2000000010	3

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Name, Address and Telephone Number:

vTech Solution Inc.
1100 H Street, N.W. Suite 750, Washington DC 20005
202.644.9774 (O)| 866.733.4974 (F)

FOR INFORMATION CONTACT THE BUYER

Jessica S Chambers
(304) 558-0246
jessica.s.chambers@wv.gov

Signature X **FEIN #** 20-4271088 **DATE** 12/13/2019

All offers subject to all terms and conditions contained in this solicitation

ADDITIONAL INFORMATION:

Addendum

Addendum No.02 is being issued to extend the bid opening date one wee to give the agency enough time to address all technical questions received.

New date and time is: 12/16/2019 at 1:30 PM (EST). .

****

The West Virginia Purchasing Division is soliciting bids on behalf of The WV Office of Technology to establish an open-end contract for an End Point Detection and Response Software to support endpoints across the state of West Virginia but can be managed centrally. This service will assist in the continuous monitoring and response to advanced cyber security threats. The open-end contract resulting from this solicitation will provide licensing for this platform, as needed per the terms and conditions and specifications as attached.

INVOICE TO	SHIP TO
	IS&C - CHIEF FINANCIAL OFFICER
DEPARTMENT OF ADMINISTRATION	DEPARTMENT OF ADMINISTRATION
OFFICE OF TECHNOLOGY	BLDG 5, 10TH FLOOR
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR	1900 KANAWHA BLVD E
CHARLESTON WV 25305	CHARLESTON WV 25305
US	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	CNTRCT ITEM: Containment Remediation Reporting & Monitoring	2000.00000	EA	$ 52.34	$104,696.00

Comm Code	Manufacturer	Specification	Model #
43233204	CheckPoint	Endpoint Protection	N/A

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

4.1.1.2 The Vendor must provide a cloud-based software as a service solution that can be centrally managed by a West Virginia Office of Technology Administrator.

For further details see attached specifications.

INVOICE TO	SHIP TO
	IS&C - CHIEF FINANCIAL OFFICER
DEPARTMENT OF ADMINISTRATION	DEPARTMENT OF ADMINISTRATION
OFFICE OF TECHNOLOGY	BLDG 5, 10TH FLOOR
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR	1900 KANAWHA BLVD E
CHARLESTON WV 25305	CHARLESTON WV 25305
US	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Opt Renew Y2 - Cntrct Item: Contain Remediate Report Monitor	2000.00000	EA	$57.34	$114,680.00

Comm Code	Manufacturer	Specification	Model #
43233204	CheckPoint	Endpoint Protection	N/A

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

4.1.1.2 The Vendor must provide a cloud-based software as a service solution that can be centrally managed by a West Virginia Office of Technology Administrator.

For further details see attached specifications.

INVOICE TO	SHIP TO
	IS&C - CHIEF FINANCIAL OFFICER
DEPARTMENT OF ADMINISTRATION	DEPARTMENT OF ADMINISTRATION
OFFICE OF TECHNOLOGY	BLDG 5, 10TH FLOOR
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR	1900 KANAWHA BLVD E
CHARLESTON WV 25305	CHARLESTON WV 25305
US	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	Opt Renew Y3 - Cntrct Item: Contain Remediate Report Monitor	2000.00000	EA	$62.00	$124,000.00

Comm Code	Manufacturer	Specification	Model #
43233204	CheckPoint	Endpoint Protection	N/A

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

4.1.1.2 The Vendor must provide a cloud-based software as a service solution that can be centrally managed by a West Virginia Office of Technology Administrator.

For further details see attached specifications.

INVOICE TO	SHIP TO
	IS&C - CHIEF FINANCIAL OFFICER
DEPARTMENT OF ADMINISTRATION	DEPARTMENT OF ADMINISTRATION
OFFICE OF TECHNOLOGY	BLDG 5, 10TH FLOOR
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR	1900 KANAWHA BLVD E
CHARLESTON WV 25305	CHARLESTON WV 25305
US	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	Opt Renew Y4 - Cntrct Item: Contain Remediate Report Monitor	2000.00000	EA	$62.00	$124,000.00

Comm Code	Manufacturer	Specification	Model #
43233204	CheckPoint	Endpoint Protection	N/A

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

4.1.1.2 The Vendor must provide a cloud-based software as a service solution that can be centrally managed by a West Virginia Office of Technology Administrator.

For further details see attached specifications.

SCHEDULE OF EVENTS

Line	**Event**	**Event Date**
1	Technical Question Deadline 9:00 AM	2019-12-02

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions