FORCEPOINT
POWERED BY Raytheon

Datasheet

Threat Protection Appliance

AN APPLIANCE-BASED SOLUTION TO DETECT AND COMBAT ADVANCED INTERNAL AND EXTERNAL THREATS ON EMAIL, WEB, AND ENDPOINTS IN REAL-TIME

FEATURES AND BENEFITS

- **Performs** network-wide monitoring to detect advanced known and unknown malware and malicious attacker behaviors, including lateral movement, typically undetected by standard security and signature-based solution defenses
- **Includes a Windows endpoint agent** that continuously monitors end-point activity across a variety of channels including: files, emails, web/webmail, removable media and IM with file/registry scanning to provide visibility to detect and remediate threats in real-time, protecting your organization from data losses and breaches
- **Incorporates advanced behavioral analytics** and attacker profiling to detect unknown threats
- **Enables** unparalleled awareness of threats through comprehensive monitoring of all inbound vectors and stopping malware reducing attacker dwell time and lateral movement
- **Provides** analytics, visualizations, and link analysis capabilities to discover capabilities and detect/combat advanced internal/external threats enabling security professionals to quickly prioritize alerts and remediate the highest priority threats in real time decreasing overall detection and escalation time
- **Scalable solution** that grows with your organization and interoperates with existing mail infrastructures to protect services, preserve investment, and reduce down-time

Organizations of all sizes today are facing unprecedented, 24/7 daily threats to their infrastructure from sophisticated, organized, and well-funded adversaries. These threat actors are often motivated by significant financial gain and sponsored by nation-states, criminal organizations, or radical political groups.

According to the 2015 Cost of Data Breach Study: Global Analysis[1] by Ponemon Institute research, businesses across all industries, including healthcare, financial services, industrial manufacturing, government, education, and media services providers, including their partner and reseller networks, are real targets for damaging cyber-attacks including data breaches. Not only do you face more advanced cybercriminals now, but also the types of information of value to them are continually expanding to include financial, information technology, operations, human resources, legal, marketing, sales, and development. All of these types of confidential information are now at risk of being compromised, modified, and electronically stolen.

These cybercriminals (a.k.a. threat actors) have the capabilities to co-opt your systems by evading signature-based detection and to stealthily exploit unknown vulnerabilities in your network for years masking them as normal operations. These malicious attacks result in intellectual property compromise, decreased operational productivity, missed opportunities, and significant impact to your organization's bottom line. At

1 2015 Cost of Data Breach Study: Global Analysis by Ponemon Institute Research, May 2015

the end of the day, through direct and indirect costs, these breaches will put in jeopardy the three most important parts of your business: your intellectual property, your customers, and your brand reputation.

It is not a matter of "if," but "when" your organization will be attacked. Will you be ready?

THREAT PROTECTION APPLIANCE OVERVIEW

Organizations require a new, more sophisticated suite of cyber products specifically designed to detect attacks of an unknown and unconventional nature in order to omit exposure and mitigate risks to your organization. Today's new breed of cyber-attacks is unrelenting. Threat Protection Appliance detects and helps to quickly combat advanced internal and external threats in real-time.

Organizations like yours trust and depend on Threat Protection Appliance to contain exposure, minimize disruptions, and protect critical organizational assets.

DEFENDING AGAINST ADVANCED PERSISTENT THREATS

Continuous Monitoring

Threat Protection Appliance provides your organization with unparalleled awareness of threats through comprehensive monitoring of endpoint activity and inbound content and incorporates advanced behavioral analytics to detect unknown threats.

Our expansive detection technology uses a variety of analytic techniques to monitor and contextualize events in real-time. For example, machine-learning algorithms are used to provide adaptive behavioral baselines and spot anomalies, while heuristic analysis is used to detect similarities to known threat signatures.

The solution employs both proprietary and third party algorithms that run in parallel. We use correlation algorithms to interpret results and determine whether something is a threat or not. As the threat landscape changes, we continue to evolve out detection algorithms.

Threat Protection Appliance includes a Windows endpoint agent that pervasively monitors the end-point across a variety of sensors including: files, emails, web/ webmail, removable media and IM with file/registry scanning to detect threats and protect your organization from data losses and breaches. Moreover, unlike other vendor products, our Threat Protection Appliance's end-point agent monitors systems resources, especially during software upgrades. It has an inconspicuous footprint and monitors threats without adverse impacts to the user experience.

Threat Protection Appliance includes an extremely robust endpoint component that simplifies deployments and lessens the need to deploy complicated SSL inspection technology.

Proprietary Hypervisor Technology

Our behavioral / sandbox analysis engine contains a proprietary hypervisor. Threat actors know that their malware is being detonated in sandboxes for analysis. Therefore, they build evasion mechanisms into their malware to detect whether it is being run in commonly deployed hypervisors. Threat Protection Appliance proprietary hypervisor technology does not leave footprints on guest operating systems, making it extremely difficult for threat actors to build effective malware evasion mechanisms.

PRIORITIZING ALERTS AND MINIMIZING EXPOSURE

Contextual Awareness

Threat Protection Appliance enables the determination of threat location (e.g., email, network endpoint breach) and the extent of the threats. The solution provides analytics, visualizations, and link analysis capabilities to discover capabilities and detect/combat advanced internal/external threats enabling security professionals to quickly prioritize alerts and remediate the highest priority threats in real-time decreasing overall detection and escalation time. It protects your most critical information assets by identifying who is accessing data, what they are accessing, when and where it is accessed, and whether the data was moved. You can determine if suspicious activities on endpoints are malicious or inadvertent (e.g., insider attacks, low-and-slow ATP, or inadvertent user error) enabling rapid forensic analysis and investigation through relational awareness.

Proprietary Visualizations and Analytics

Threat Protection Appliance has an intuitive user interface allowing analysts to quickly prioritize alerts and remediate the highest priority threats in real-time decreasing overall detection and escalation time.

UNDERSTANDING THE THREAT LANDSCAPE

Comprehensive Visibility
Threat Protection Appliance's comprehensive visibility into endpoint actions and inbound/outbound files enables your security professionals to understand their security posture and to assess the effectiveness of their defense.

Complements Existing Email Controls and Enables Interoperability
Threat Protection Appliance enhances traditional signature based email filtering technologies such as anti-spam and anti-virus to prevent malicious content.

ENTERPRISE SCALE AND INTEROPERABILITY

Enterprise-Scalability
Threat Protection Appliance has been deployed within large organizations and scales to tens of thousands of endpoints, millions of emails, and gigabits of network traffic.

CONCLUSION

Threat Protection Appliance protects your organization against advanced internal and external threats in real-time. This enables your security professionals to prioritize and quickly remediate and contain threats and breaches. Global organizations just like yours trust and depend on our Threat Protection Appliance to contain exposure, minimize disruptions, and protect critical organizational assets.

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

[DATASHEET_THREAT_PROTECTION_APPLIANCE_EN] 100041.011416