UNISYS

Securing Your Enterprise Against Advanced Persistent Threats

Freedom To Focus On What Matters Most – Your Business

Safeguard your Critical Information from Advanced Threats

Present day enterprises must navigate a multitude of security, budget, and compliance challenges that are drawing focus and resources away from their missions. Disruptive trends such as Mobile, Cloud, Big Data and Smart Computing have introduced myriad security challenges for almost every enterprise. Securing data in the clouds while enabling mobile access is a necessary efficiency as supply chains are integrated, and adversaries are both skilled and motivated to attack.

Recently enterprises and government agencies have fallen prey to varied, successful cyber-attacks of unprecedented sophistication and reach. Conventional Corporate IT network security implementations with "protect-the-perimeter" approach where multiple layered security defense controls are deployed, are not sufficient to combat presentday advanced threats.

HIGHLIGHTS

- 80-90Mn Security threats occur annually and are estimated to cost $2.1Tn annually by 2019 [1]
- Advanced Persistent Threats and Polymorphic Malware are dynamic, adaptive, easily compromises today's defenses
- Regulatory compliance, vulnerability exploits and Target breaches are key security drivers for CISOs [2]
- 77.9% of CISOs had to assume responsibility for a breach [2]

1. Source: Bank of America Merrill Lynch
2. Source: IDC's State of the "C" in CISO Survey, 2015

The Accelerated Rate of Cybersecurity Incidents

2015 was known as "The Year of Cybersecurity Incidents." However, this isn't much different from what we saw in 2014, and 2013 and 2012. Each time the public is exposed to a "massive breach," it is bigger and more destructive than the previous. In June 2015, the U.S. government's Office of Personnel Management (OPM) reported that background check data for millions of Americans had been compromised. For decades, the rapid expansion of technology and its integration into every part of enterprises has contributed to improved service delivery and efficiency – most recently through cloud and mobile. But this rapid technology integration comes at a cost – as indicated by Operation Shady RAT, where an APT attack stole intellectual property from 70 government agencies across 14 countries.

Across all of the recent attacks, there is one common thread: the bad guys always get in. Today's attacks get in, then move around, and then start doing damage. The attack vectors vary greatly, from social engineering to Advanced Persistent Threats to something as simple as an unpatched server or a lost laptop. How can Security Leaders battle sophisticated threats & rising costs at the same time?

The Need for a Different Approach

Next generation of cyber-attacks, such as APTs and polymorphic malware are dynamic, adaptive, stealthy and extremely successful at compromising today's defenses. In-order to prevent these motivated adversaries from attacking systems, stealing data, and harming critical infrastructure, enterprises ought to think differently. They must realize the limitations of traditional signature-based defenses and leverage new technology to uncover and stop today's new breed of cyber-attacks. Unisys is introducing Advanced Threat Protection (ATP) service, an innovative new security threat detection and prevention platform proven to help win the war against next-generation threats.

Unisys Advanced Threat Protection Services (ATP)

Unisys Advanced Threat Protection (ATP) service, is an innovative security threat detection and prevention solution powered by FireEye® Threat Prevention Platform coupled with Unisys patented UNCAAP technology and our deep expertise in the field of Incident Management. This powerful synthesis of technology, services, and Dynamic Threat Intelligence (DTI) can safeguard corporate assets in real time.

It has four major components - Malware Defense Service, Advanced Persistence Threat Defense Service, Malware Forensics Service and Threat Consulting Service.

Malware Defense Service (MDS) - MDS provides comprehensive defense against web, email, and content-based malware attacks. It flows within the environment in scope to hunt for malicious content and if found, performs a detailed analysis in the dynamic MVX engine.

Advanced Persistent Threat Defense Service (APTDS) - APTDS focuses on helping government/federal clients who are under constant APT attacks. It combines our existing managed security service and MDS to provide proactive defense against the APTs. We also integrate our SIEM UNCAAP technology for early detection of attacks.

Malware Forensics Service (MFS) - Unisys MFS detects the lifecycle of active malwares. Our security analysts and researchers study the Malware behavior by analyzing the IOC and develop a counter-defend strategy.

Threat Consulting Service (TCS) - TCS provides a detail report on the threat landscape of our clients with the aim of flagging out gaps that can be targeted by the advanced threats.

"With Unisys' proprietary state of the art micro-segmentation technology and world class physical security and biometrics products, Unisys Managed Security services are designed to be identity based instead of device based, ensuring incremental security protection and synergies."

Frost & Sullivan

Unisys ATP Helps Enterprises:

Enhance Security & Minimizes Risk by:

- Identifying and detecting cyber-attacks that normally bypasses signature-based tools and common sandboxes based solutions
- Holistic protection against inbound attacks, outbound callbacks, and malware executable downloads
- Understanding entire context of advanced attacks using FireEye's multi-flow analysis, whereas other point products see only a single attack flow

Reduce Time and cost by:

- Leveraging FireEye's Threat Intelligence data, which is shared in real-time locally and globally via the DTI Cloud
- Proactively monitoring system health to ensure continued detection efficacy and critical alerts from our intelligence experts
- Automatically containing compromised devices and providing in-depth analysis of infected systems and detailed actionable recommendations for threat protection

UNISYS

For more information on our ATP services, please visit: www.unisys.com/mss

© 2016 Unisys Corporation. All rights reserved.

Unisys and other Unisys product and service names mentioned herein, as well as their respective logos, are trademarks or registered trademarks of Unisys Corporation. All other trademarks referenced herein are the property of their respective owners.

Printed in the United States of America 04/16 16-0177 (a)