Galaxite solutions

WHITE PAPER

ENDPOINT PROTECTION: THE BENEFITS OF HOLISTIC SECURITY

CONTENTS

THE CURRENT THREAT LANDSCAPE

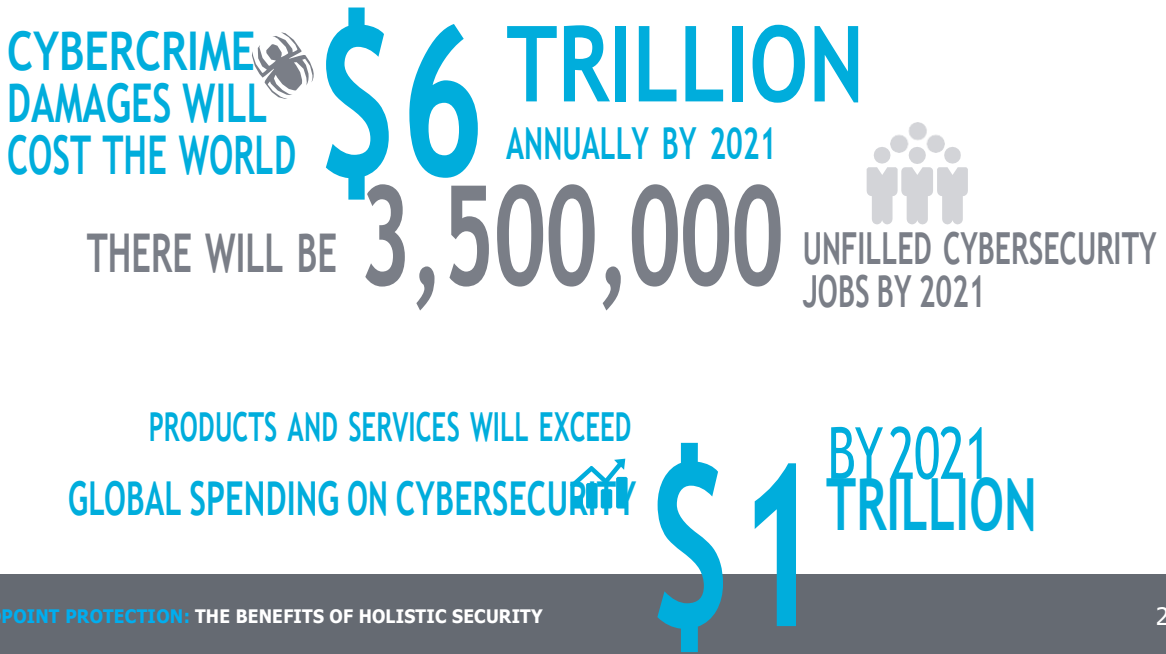
IT security has gotten out of hand. Governments are being infiltrated. Businesses are being penetrated. Hospitals are being held ransom and ordinary people are being terrorized.

Impacted by the ongoing and constant parade of attacks, many enterprises focus on protecting themselves against the latest perceived threats while failing to assess if they are actually vulnerable. It's the Cyber Wild West.

CISOs Struggle to Manage
CISOs, the designated sheriffs of the Cyber world – are struggling to continuously increase their arsenal of solutions. The life of a CISO has become increasingly difficult, with CISOs needing to deal with a multitude of issues and questions that affect and jeopardize their position on a daily basis. Questions like which new technologies to deploy in order to create maximum impact.

Quick Fixes vs. Multiple Solutions
Historically, CISOs have been in an ambiguous situation relating to managing cybersecurity matters. On one hand, CISOs focused on one dimensional quick fixes with little consideration about how they would function within the context of their existing solutions. On the other hand, some CISOs piled up multiple security solutions with the hope that the more-the-merrier approach would stop attacks.

Stockpiling Security is Creating a False Sense of Security
In this light, organizations are searching far and wide for the next security solution to purchase. A leading research organization covering the global cyber economy estimates that "global spending on cybersecurity products and services will exceed $1 trillion cumulatively over the next 5 years from 2017 to 2021." It's a security arms race that has companies purchasing the hottest new products - continuously adding and stockpiling their security arsenal - and deploying these weapons liberally. However, this blanket approach to security can lull organizations into a false sense of security. It is not viable in the long term, as already proven by attacks making the news every day.



"AN AVERAGE ORGANIZATION HAS BETWEEN 30-50 SECURITY SOLUTIONS. IT'S CRAZY TO INSTALL, MANAGE AND MAINTAIN SO MANY MULTIPLE SOLUTIONS".

SOURCE: LISA O'CONNER, MANAGING DIRECTOR - SECURITY, ACCENTURE, JULY 2017

THE CHALLENGES OF MULTIPLE SECURITY SOLUTIONS

Throwing everything at threats has not reduced Cybercrime. Many enterprises have a multitude of security controls (such as SIEM, DLP, web gateways, network access control), but each of these provides an incomplete and siloed perspective. As organizations become saturated with additional security solutions, more problems are sometimes created than are addressed.

The Dangers of the "Security Lull Effect"
Navigating today's security concerns while being bogged down by a horde of security software can create a "security lull effect." When organizations become bloated with security solutions, often the reverse occurs, and the multitude of security solutions actually become ineffective in preventing and mitigating threats.

Who's Got Time for Installation, Deployment and Maintenance?
Piling on security solutions requires extensive time to install, update, deploy and maintain - stretching IT and admin teams thin, while generating massive logs of security alerts and data. The chronic lack of qualified and experienced Cybersecurity professionals makes this time issue even more challenging for organizations.

The Danger of Missed Warnings and Misconfigurations
Multiple deployed solutions leave IT Managers, security and risk professionals piecing together a puzzle without a wide-view. Buried by thousands of alerts from different silos, security analysts struggle to connect the dots, and have no process for managing real threats — leading to missed warnings and security misconfigurations.

THE MARKET SHIFT TO A HOLISTIC PLATFORM

Enterprises do not want multiple solutions as part of their systems. Instead they want consolidation. They know they need to protect their endpoints with prevention. And detection. And response. But they want them all in one single solution. IT teams and SOC managers are looking for a robust solution coupled with simplicity and efficiency.

Instead of contracting with several different vendors for dissimilar security solutions, organizations are eager for a solution that combines the most effective security capabilities in one holistic solution. There is a real need for a single platform that integrates well with existing applications and technologies and won't slow them down.

THE BENEFITS OF A HOLISTIC SOLUTION

EASIER MANAGEMENT

Staying on top of so many different vendor products and their functions can prove to be a struggle for any security team. It can take days to update all endpoints to protect them from new malware or threats. Add-ons, moves, and changes to security devices can take weeks, with much manual intervention required to re-implement policy and ensure constant compliance.

The good news for IT professionals is that the management workload can be alleviated with one comprehensive, holistic security solution. Security changes can then be automated to flow through the network, saving valuable time.

REDUCED COSTS

Cost savings as a benefit of consolidation may not be at the top of management minds for a simple reason: they've already made the security purchase. If it's a hardware-based solution, they've bought the appliance device. If it's software-based, they've purchased the license - returning them is not an option. But what is often overlooked is that the cost of a security product doesn't end at the purchase; much of it comes from the ongoing maintenance and service renewals. Once you've consolidated and eliminated the need for a product, you can also put an end to the renewal and service expenditures that go along with it.

EFFECTIVE THREAT RESPONSE

With so many different security technologies, it's difficult to know if whether you truly have 100% visibility across your entire network. A huge challenge for organizations is having to sift through separate reporting tools and management consoles in order to try and get the full picture of what is happening. This explains how complex and advanced threats are able to remain inside a network for months without being exposed.

A holistic security framework allows for a unified management platform to monitor, manage, and orchestrate solutions across the entire distributed network. An integrated system can automate the processing and analysis of threat information from multiple sources, and can quickly identify and mitigate network security threats. The identification, isolation, and analysis of suspicious files can even be automated. All of this, if done manually, is extremely labor-intensive and time-consuming.

As enterprises continue to transform, so too will their networks and security needs. In order to keep up with the evolving complexity of today's cyber threats, organizations must simplify. By scaling down unnecessary, redundant security devices and integrating what remains within a single unified system, enterprises can make their cybersecurity solutions more effective than ever.

GALAXITE – MAKING SECURITY SIMPLE

The Galaxite 360 platform simplifies enterprise security by providing a holistic answer to all the organization's protection and prevention needs. What Galaxite does is consolidate multiple IT security capabilities into a single offering, making IT securityposture simple and easy to manage.

Galaxite 360 reduces security spend by providing multiple capabilities in a single solution, while putting less drain on organizational resources, manpower and budget. The 360 platform provides the highest level of enterprise security by correlating indicators across systems - increasing visibility and accuracy of detection throughout the organization, without the need for multiple cybersecurity solutions.

The Galaxite 360 platform launches across tens of thousands ofendpoints. Its "Big 4" correlation engines analyze and correlateindicators across the network, files, users and endpoints, issuing risk rankings for potentially anomalous behavior, ensuring lowest false positives and achieving a clear picture
of attack operations over time. Galaxite 360's machine learning and automated remediation capabilities mean processes are streamlined, putting less strain on IT security staff, enabling them to prioritize and respond to what really matters.