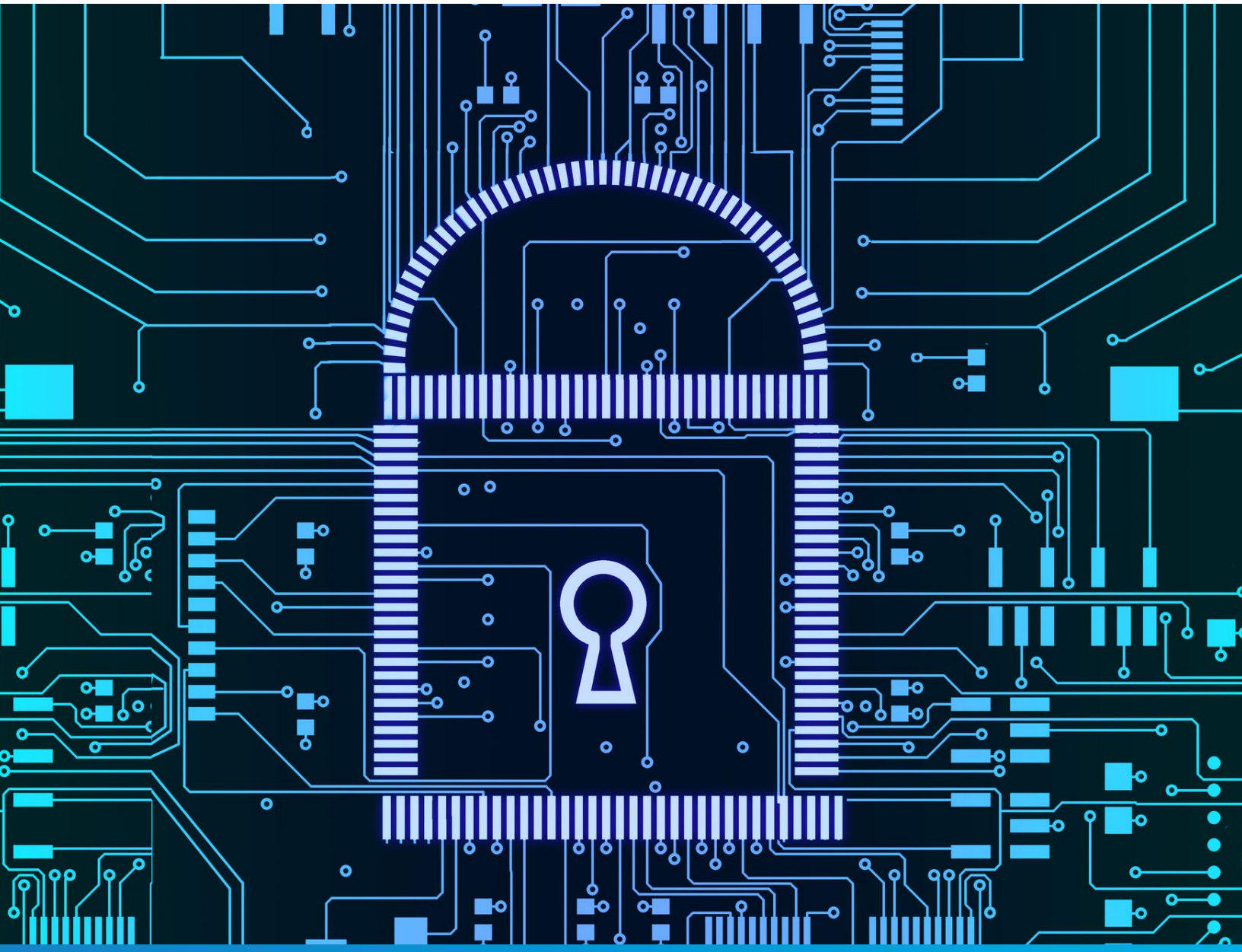
A Frost & Sullivan White Paper



Automated Breach and Attack Simulation: The Cost and Risk Reduction Revolution is Here

Jarad Carleton, Global Program Leader, Cybersecurity, and
Swetha Krishnamoorthi, Industry Analyst, Cybersecurity

FROST & SULLIVAN
The Growth Pipeline™ Company

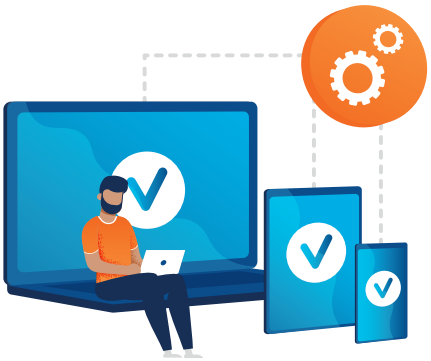
Contents

INTRODUCTION

Chief information security officers (CISOs) are facing the biggest challenge of their careers: building resilient, impenetrable, and user-friendly IT environments in their organizations.

Businesses have a growing number of endpoints connected to their devices. Frost & Sullivan estimates that there were 2.32 billion endpoints globally in 2019.[1] For an enterprise, the sheer volume of endpoints connected to its network expands its attack surface; keeping track of these endpoints is an enormous task for security teams.

ATTACK SURFACE EXPANDS AS ENDPOINTS GROW IN NUMBER

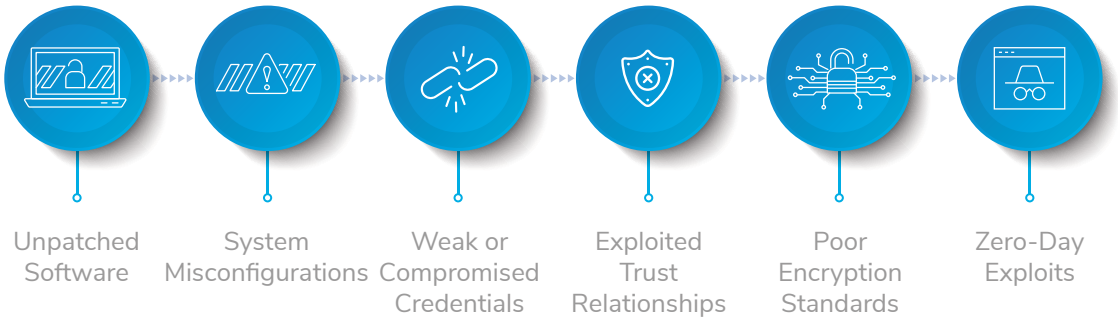


Frost & Sullivan estimates that there were **2.32 billion endpoints** globally in 2019.[1]

Source: Frost & Sullivan

In a dynamic IT environment, new security vulnerabilities crop up frequently. Data breaches are often the consequence of vulnerabilities arising from unpatched software, system misconfigurations, weak or compromised credentials, exploited trust relationships, poor encryption standards, or zero-day exploits. In addition to commonly known vulnerabilities, continuous changes in the user environment can lead to misconfigurations that are at the root of many security vulnerabilities.

THE MULTIPLE PATHS TO A DATA BREACH



Source: Frost & Sullivan

Enterprises also need to ensure the security of employees' personal devices as a result of government stay-at-home orders issued to contain the COVID-19 pandemic. Although the concepts of bring your own device (BYOD) and remote work are not new, they have become the

1. Endpoints include laptops, desktops, notebooks, tablets, smartphones, and similar devices connected to the enterprise network.

new normal. Without adequate security systems in place, the cyber risk resulting from an increase in BYOD and remote workers could increase substantially.

The ability of a cyber adversary to attack or access business-critical assets is a direct result of the security posture of an enterprise network. However, the high volume of user activity across numerous endpoints increases the challenge of identifying issues that could unintentionally increase cyber risk for the organization and allow cyber adversaries to slip by undetected.

Businesses can minimize the impact of a data breach by continuous monitoring and real-time analysis of their network environment for vulnerabilities that can provide unauthorized access to critical assets.

MANUAL PENETRATION TESTING LIMITS

Businesses are embracing digital transformation to gain a competitive advantage. In response, IT architectures are evolving to adapt to new business priorities, processes, and policies. Yet, enterprises seldom have real-time visibility into the operational effectiveness of their security controls.

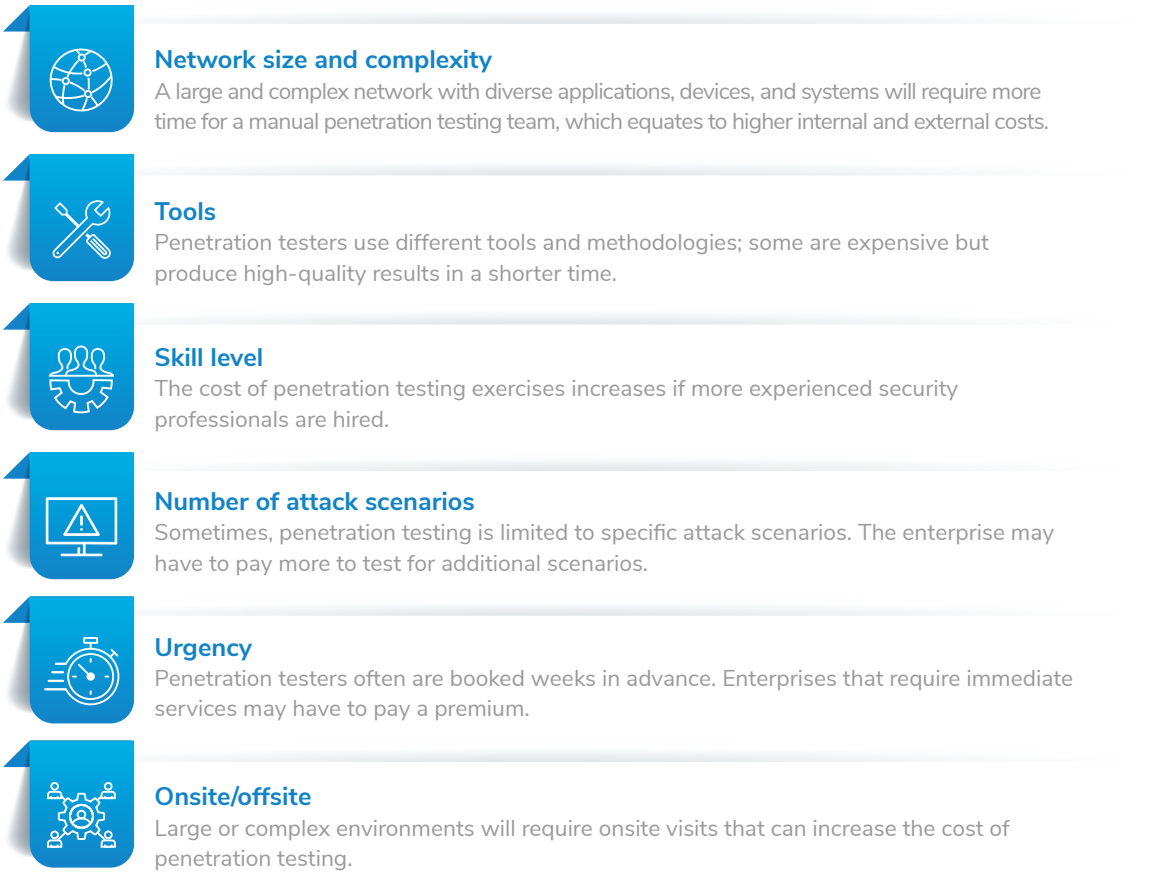
Vulnerability scanning is one of the processes used to determine an organization's security posture. It helps reduce enterprise cyber exposure by providing a long list of network vulnerabilities. However, vulnerability scanning tools seldom provide attack or risk context. As a consequence, security analysts can find it challenging to prioritize discovered vulnerabilities to take remediation steps.

Penetration testing, or pen testing, is another widely used security testing program. It attempts to discover as many vulnerabilities in the network as possible and exploit them to determine the risk and impact levels; processes can range from specific and focused application-level tests to generic ones usually done for compliance purposes.

The effectiveness of pen testing procedures relies on the expertise of the security analyst; for this reason, enterprises often hire external teams that have highly skilled professionals to conduct capture-the-flag exercises. Unfortunately, the internal security team cannot focus on other security activities, even if it outsources penetration testing: internal team members have to be available alongside the pen testers during exercise and remediation phases. Most organizations' security teams are resource-constrained, typically juggling multiple responsibilities; scheduling pen testing exercises depends on the availability of internal analysts, ultimately limiting the frequency to one or two times a year.

When pen testing exercises are scheduled twice a year, they generally include one with a broad focus and another with limited scope. Manual penetration tests, however, only provide a snapshot of a specific moment in time of a large organization's IT infrastructure; the exercises can prove ineffective in capturing critical vulnerabilities in a fast-changing IT environment.

PENETRATION TESTING COSTS VARY, DEPENDING ON THE FOLLOWING FACTORS:



Network size and complexity
A large and complex network with diverse applications, devices, and systems will require more time for a manual penetration testing team, which equates to higher internal and external costs.

Tools
Penetration testers use different tools and methodologies; some are expensive but produce high-quality results in a shorter time.

Skill level
The cost of penetration testing exercises increases if more experienced security professionals are hired.

Number of attack scenarios
Sometimes, penetration testing is limited to specific attack scenarios. The enterprise may have to pay more to test for additional scenarios.

Urgency
Penetration testers often are booked weeks in advance. Enterprises that require immediate services may have to pay a premium.

Onsite/offsite
Large or complex environments will require onsite visits that can increase the cost of penetration testing.

Source: Frost & Sullivan

With so many variables, businesses often prioritize segments of their infrastructure for manual penetration testing to control costs. A single penetration testing exercise can cost between $10,000 and $100,000, depending on the scope.

Besides cost, a key concern with penetration testing exercises is that they can be disruptive for the production environment. Penetration testing is inherently invasive since it employs techniques similar to those used in a real attack. Manual penetration testing exercises have a reputation for breaking systems, knocking business-critical production systems offline, or inadvertently exposing confidential information.

Suffice it to say, when penetration testing goes wrong, it is a business disruptor. When fragile infrastructure is knocked offline, downtime of just a few hours can result in severe service interruptions and substantial revenue loss for an enterprise and its customers in addition to the cost associated with rebuilding the affected systems.

For instance, a service interruption at during a manual penetration test exercise at one organization unintentionally took down logistics services for 2.5 hours, at a cost of €100,000 per hour for that system alone. A few smaller systems were impacted as well, adding to the overall expense.

Penetration testers collect a lot of data during the exercise; compilation, analysis, and presentation of data can take between two and seven days to complete, depending on the scope of the exercise. In addition, as previously mentioned, a pen testing exercise can only focus on a discrete portion of the organization's IT infrastructure. Thus, the security team gets only a narrow and frozen snapshot from a subset of a much larger IT infrastructure.

Every network continues to evolve after that snapshot is taken, and so does an enterprise's security posture. Meanwhile, the report from the exercise can take up to six months to review and remediate identified deficiencies. By the time the security team finishes the remediation steps for identified vulnerabilities, the IT environment will have already changed.

SECURITY GAPS WIDEN WITH REMOTE WORKING

The COVID-19 pandemic has disrupted the world in many ways, but a direct impact on business has been the rapid acceleration of the remote worker trend. Many businesses, ranging from technology giants to local retail shops, have allowed and, in many cases, issued mandates to work from home (WFH). In just one fiscal quarter, businesses began to experience the security impact of this transition.

The shift in business operations quickly exposed deep and significant cracks in enterprise security. For example, not all businesses and organizations were able to supply enough company-issued laptops with centralized IT management and security tools to their WFH workforce. In many instances, companies have had to rely on personal, unmanaged smartphones, tablets, laptops, and desktop PCs that lacked enterprise-class security protections. As this occurred, a well-known security issue began to impact businesses on a broad scale for the first time: most home networks are not adequately secured.

Although the WFH trend has substantial business benefits for a post-COVID-19 world, accelerated provisioning inevitably results in misconfigurations and overlooked security policies and controls. Without proper systems in place for WFH business environments, security teams will not have sufficient visibility of the security hygiene for all endpoints, including servers. Endpoint detection and response (EDR) tools used by enterprises may not be configured for virtual work environments, further degrading endpoint visibility and insight into an organization's security posture.

As a consequence, the risk of an attack increases as undetected vulnerabilities lurk in the system and, in some cases, provide unauthorized access to critical business assets.

BEST PRACTICE: AUTOMATED BREACH AND ATTACK SIMULATION

Manual penetration testing exercises can lead to unintended collateral damage to business systems, can fail to discover all potentially vulnerable paths to critical business assets, and are unable to cost-effectively test large, complex networks. Today's dynamic IT and business environment requires real-time visibility into the security posture of the company. While penetration testing can give a snapshot of the security posture at a specific point in time, businesses find it hard to assess their cyber risk as the network

changes. Often, security teams have to wait six months to one year until the next penetration testing exercise to identify new vulnerabilities.

Automated breach and attack simulation (BAS) tools are an effective and proven alternative to manual penetration testing exercises. BAS tools help enterprises improve their security posture by running continuous penetration testing of IT infrastructure, acting like a real attacker but avoiding collateral damage to business-critical systems.

Automated BAS tools help enterprises keep pace with a cyber adversary's breach methods and ever-evolving enterprise networks. These tools monitor systems around the clock without knocking systems offline. They can identify previously undiscovered vulnerabilities and map multiple vulnerable paths to critical assets without compromising the continuity of critical production environments.

With continuous scanning, BAS tools allow CISOs and security teams to keep their finger on the security pulse of the organization in real time. An advanced BAS tool should always include a mapping feature of the exposed endpoints, servers, or systems for the security team to easily understand all vulnerable paths to any endpoint or business system. This allows security teams to fix vulnerabilities as soon as they arise and maintain a higher level of security hygiene than was previously possible.

BAS tools allow CISOs and security teams to keep their finger on the security pulse of the organization in real time.

Penetration testing exercises may require at least two security analysts from the internal team in addition to the team of external penetration testers. If a pen testing exercise goes on for five days, the CISO may have to spend upward of $50,000 for a group of three external pen testers and two internal security analysts.

Conversely, BAS tools require minimal human involvement. A cloud-based agent deployed on endpoints works to identify vulnerabilities and updates security teams continuously and in real time. With an advanced BAS solution, the dashboard will recommend subsequent remediation actions and can integrate with security information and event management (SIEM) or security orchestration and response (SOAR) platforms.

Besides the initial investment for the platform, the CISO doesn't need to spend additional money on external security assessments. BAS tools help enterprises scale up their security posture assessments, regardless of the size or complexity of the network. They can also continuously conduct security risk assessments across the entire network infrastructure. Accomplishing the same task with manual penetration testing would require millions of dollars annually.

The exhibit below compares the cost difference for three manual penetration tests per year versus an automated BAS system.

PENETRATION TESTING COSTS VARY, DEPENDING ON THE FOLLOWING FACTORS:

Variables	Manual Penetration Testing	Automated BAS
Penetration Tests per Year	3	3
Endpoints per Test	5,000	5,000
External Pen Testers	5	0
External Labor Hours per Test*	800	0
External Labor Hours for Reporting**	400	0
Internal Security Analysts	2	1
Internal Labor Hours per Test***	160	40
Cost per Labor Hour External****	$234	$0
Cost per Labor Hour Internal	$48	$48
Average Retail Price of BAS per Endpoint	$0	$75
Cost of Annual Pen Tests	**$865,440**	**$376,920**
Average Pen Test Cost per Endpoint	**$57.70**	**$25.13**

Source: Frost & Sullivan

Important points to consider from the comparison chart are:

1. Manual penetration testing may only find one or two paths to critical assets
2. Automated BAS runs around the clock to find every vulnerable path to critical assets
3. Every additional manual penetration test of the same scale adds $288,480 to annual costs and the average pen test cost per endpoint remains $57.70
4. Every additional BAS pen test adds $1,920 to annual costs and the average pen test cost per endpoint drops by several dollars. For example: 10 BAS pen tests have an average pen test cost per endpoint of $7.54

XM CYBER: AUTOMATED BAS WITHOUT ENDANGERING NETWORK PRODUCTION ENVIRONMENTS

XM Cyber, founded by three senior executives from the Israeli intelligence community, has a unique, cloud-based, automated BAS platform that mimics cyberattacks on endpoints to identify security vulnerabilities without compromising on safety, accuracy, or business continuity.

XM Cyber's BAS platform includes two engines:

a. The red team engine continuously simulates sophisticated cyberattack techniques to identify weaknesses in IT infrastructure.

b. The blue team engine analyzes the attack vectors identified by the red team engine and helps enterprises prioritize remediation steps.

The red team engine performs numerous attack scenarios targeting assets defined by the customer. The solution runs continuously on the system, targeting the defined assets, and provides the user with a prioritized remediation report.

The platform has several pre-defined attack scenarios, such as customer data, network superiority, IT/OT integration, financial server protection, ransomware impact, and corporate intellectual property. The dashboard displays each endpoint in the network as an icon on a network map.

As the simulation begins, some endpoints are quickly identified as vulnerable; however, as the simulation proceeds, more vulnerable endpoints are identified as different attack techniques are tested on numerous paths as it pivots and uses every path possible to reach the defined critical assets.

XM Cyber's platform mimics a real cyber adversary and conducts reconnaissance in the network and, eventually, inside secure zones.

XM Cyber's platform mimics a real cyber adversary and conducts reconnaissance in the network and, eventually, inside secure zones. At the end of the simulation, the enterprise can view the number of critical assets compromised and track each attack vector and its path to the defined critical assets. The enterprise security team is then able to investigate each step leading to the simulated breach and determine whether one or more chokepoints can be addressed to protect secure zones.

The blue team engine considers the criticality of the asset and severity of the impact in its suggested prioritization of remediation action items. For instance, a compromised server may have a low vulnerability ranking; however, by harvesting credentials on the server, cyber adversaries may be able to continue lateral movement across the network and reach critical business assets. With this context, the security teams can maximize the efficacy of their remediation steps, which is important for resource-constrained organizations. This level of holistic analysis requires complete visibility of the enterprise network from the attacker's perspective. XM Cyber, armed with a thorough understanding of the customer's network, can provide actionable and specific recommendations to rapidly strengthen security hygiene organization-wide.

XM Cyber, armed with a thorough understanding of the customer's network, can provide actionable and specific recommendations to rapidly strengthen security hygiene organization-wide.

The platform includes a dashboard that summarizes the entire network environment and provides a quantitative security rating of 1 through 5, based on its continuous real-time findings in the customer's environment.

CASE STUDY

One of the largest ports in Europe is responsible for the maintenance of the harbor area, railway infrastructure, and flood protection. The port has approximately 2,000 employees and owns facilities to handle bulk cargoes of thousands of logistics companies.

Problem

The port has approximately 3,500 endpoints that include workstations and servers. Of its five cybersecurity specialists, three work part-time on operational security processes; two full-time security analysts are responsible for designing security policies.

The company conducted manual penetration testing exercises twice a year, but the exercises all too frequently resulted in collateral damage to business-critical systems and service interruptions. Depending on the type of interruption, downtime ranged from one to three hours. In addition to the cost of penetration testing, the company had to spend significant time and effort to rebuild the systems damaged by manual penetration test exercises. Further, the report creation took more than a week and remediation steps needed almost six months to address following the penetration test. More importantly, the company was never able to get clear insight into the security hygiene of the entire network because the exercises were only focused on a subset of its larger IT infrastructure.

Solution

The company ran a proof-of-concept trial with XM Cyber's automated BAS platform, simulating penetration testing across its infrastructure while averting any possibility of collateral damage. Running a wide variety of hacking scenarios again and again allowed the company to identify multiple business-critical vulnerabilities that previous penetration tests had not.

XM Cyber collected all the data with lightweight sensors that were quickly and easily placed on endpoints. The platform was even able to find small but important pieces of data on endpoints such as access lists and other files that could be leveraged by a real attacker to advance an attack.

"No administrator is going to look at fifth-level folders to check access rights on a folder. It would never be done manually. XM Cyber did find it and revealed that everyone in the company had rights to a folder that should have been restricted. With 10 or even 20 administrators, it's nearly impossible to find something like this."
– CISO of a major European Port

Impressed by the XM Cyber team's depth and breadth of knowledge about IT infrastructure and the cost-savings it offered, it was an easy business case for the CFO to approve.

THE FINAL WORD

An organization's information security goals regularly change as new and more sophisticated threats emerge. Frequent updates to business policies, processes, and objectives combined with configuration changes and security updates also regularly introduce new vulnerabilities in the IT environment.

Frost & Sullivan research shows that enterprises with real-time, 360-degree visibility and contextual understanding of vulnerabilities in their IT environment are far better positioned to mitigate serious threats. Yet, manual penetration testing exercises only give a point-in-time snapshot of a small part of the IT environment, and the findings lose relevance quickly. In addition, the high cost of manual penetration testing and the high probability of collateral damage deter more frequent penetration testing exercises.

Automated BAS tools such as XM Cyber change this equation and enable organizations to continuously monitor their IT environment for vulnerabilities in a safe, scalable, and cost-effective manner as the network changes. Since minimal input is required from security analysts, IT teams can focus their efforts on other critical tasks.

Frost & Sullivan believes that leveraging advanced automated BAS technology is a best practice that more enterprises with a large number of endpoints need to embrace. It will unquestionably enable organizations to raise the bar on security hygiene while simultaneously allowing IT departments to become more efficient.

NEXT STEPS

- **Schedule a meeting with our global team** to experience our thought leadership and to integrate your ideas, opportunities and challenges into the discussion.
- Interested in learning more about the topics covered in this white paper? Call us at 877.GoFrost and reference the paper you're interested in. We'll have an analyst get in touch with you.
- Visit our **Digital Transformation** web page.
- Attend one of our **Growth Innovation & Leadership (GIL)** events to unearth hidden growth opportunities.

Silicon Valley
3211 Scott Blvd, Suite 203
Santa Clara, CA 95054
Tel 650.475.4500
Fax 650.475.1571

San Antonio
7550 West Interstate 10
Suite 400
San Antonio, TX 78229
Tel 210.348.1000
Fax 210.348.1003

London
Floor 3 - Building 5,
Chiswick Business Park
566 Chiswick High Road
London W4 5YF
Tel +44 (0)20 8996 8500
Fax +44 (0)20 8994 1389

myfrost@frost.com 877.GoFrost http://www.frost.com

FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?