Strengthening networks and endpoints with behavior-based protection

Disrupt mutating threats in real time with intelligent, end-to-end security solutions from IBM
Introduction

Thanks to hackers’ relentless use of multiple attack methods, security breaches are more common than ever. In 2013 alone, more than half a billion records of personally identifiable information—including names, email addresses, credit card numbers and passwords—were stolen.¹ And the attacks have taken place in virtually every industry.

To help protect against the latest advanced threats, many organizations have opted to augment their traditional perimeter defenses (firewalls and anti-virus tools) with point solutions focused on threat detection. But these point solutions often target a single threat vector, leaving the organization exposed to other attacks. By contrast, protection that is based on the behavior of malware and malicious actors within an organization’s network can effectively mitigate a wide range of attacks, including zero-day threats that exploit a previously unknown vulnerability.

This white paper will explain how organizations can use behavior-based protection strategies to fight the latest threats, including zero-day attacks. It will look at how an integrated, intelligent approach to threat prevention, not just detection, can break the attack chain—and disrupt malicious attacks in real time. In addition, it will introduce network and endpoint security solutions from IBM that make it easy to deploy, manage and maintain behavioral protection within your organization.

Breaking the attack chain

Traditional methods of defense have failed again and again at protecting organizations against the latest advanced, multilayered attacks.

Today’s attacks typically involve this chain of events:

- **Break in**: An unsuspecting user can click a link in a phishing email, sending an exploit to the browser.
- **Latch on**: A remote employee opens an attachment, which tries to download and install malware.
- **Expand**: Once inside the network, malware searches for ways to elevate the attacker’s privileges to access critical systems.
- **Gather**: Malware on an internal system attempts to access and export data from critical resources.
- **Exfiltrate**: Running on a supposedly protected system, malware attempts to quietly siphon out data.

To disrupt this attack chain to help prevent breaches, organizations need to be able to both detect and prevent unusual behavior—from the network perimeter to the core endpoints (physical and virtual, on-premises and remote). However, many security point solutions are designed to block specific exploits, requiring different “signatures” to match the different patterns of a single exploit. As new variants of the exploit appear, new signatures must be created; and each new signature can impact the overall network and endpoint performance.

Zero-day threats are particularly problematic for signature-based protection, due to a lag between the malware attack and the deployment of the signature. What’s more, advanced persistent threats are constantly mutating, so they no longer match the pattern of a known exploit. In fact, they are specifically designed to evade anti-virus and signature-based protections.
Deploying behavior-based protection

To overcome the security gaps that result from multiple point products, as well as the limits of exploit-based protection, organizations need network- and endpoint-focused security solutions that can help detect malicious behavior in real time—ideally, when it can be stopped and prevented.

IBM Security solutions support a behavior-based approach to security that can help block even unknown attacks, including those utilizing advanced malware. The IBM® Security Network Protection (XGS) appliance helps prevent attacks from reaching vulnerable hosts, while IBM Security Trusteer® Apex™ Advanced Malware Protection disrupts the installations of malware on users’ computers. These solutions also work in tandem to help block attackers from establishing external control channels.

Protecting the network

Going beyond simple pattern matching on known signatures, IBM Security Network Protection includes multiple layers of prevention technologies to offer broad coverage from known threats, while also effectively addressing new threats as they emerge. Some of the key capabilities that allow it to block constantly mutating threats include:

- **Vulnerability decodes**: Algorithms that help protect against attempts to exploit the vulnerability instead of matching on well-known exploits
- **Application-layer heuristics**: Heuristic-based decodes that analyze application protocols and identify behavior consistent with attacks
- **Web injection logic**: Analysis of web traffic with the ability to block zero-day SQL injection, cross-site scripting and command-injection attacks
- **Shellcode heuristics**: Heuristic-based decodes that detect shellcode in commonly used file and network protocols
- **Content analysis**: Inspection of files and documents for non-conformance and malicious content
- **Protocol anomaly detection**: Stateful packet inspection of network and application protocols to identify non-conformance and malicious behavior

---

Spectrum of vulnerability and exploit coverage

![Diagram showing spectrum of vulnerability and exploit coverage]

IBM stays ahead of the threat with these prevention methods

Many intrusion prevention solutions stop here

Exploit signatures—pattern matching
Strengthening networks and endpoints with behavior-based protection

IBM Protocol Analysis Module (PAM)—designed and updated by the IBM X-Force® research and development team—is a key behavioral protection element within the IBM Security Network Protection appliance. The X-Force team tracks Internet threat levels from its Global Threat Operations Center to create the world's most comprehensive threat database. X-Force then incorporates protection into PAM and provides security updates in order to help security professionals stay ahead of emerging threats.

Supported by PAM and the X-Force database, IBM Security Network Protection empowers organizations to protect against zero-day exploits and proactively identify a wide range of security risks, such as malware, botnets, peer-to-peer activity and many others. To help ensure accurate, preemptive protection against threats, the solution also includes support for more than 2,000 applications and individual actions, and leverages a database of more than 23 billion URLs. IBM web-crawling technology continually categorizes and re-categorizes URLs to keep the vast database up to date.

As a result, IBM Security Network Protection has proven to be tremendously effective in preventing advanced threats, sometimes months or even years before the discovery of a given vulnerability.  

For endpoints, Trusteer Apex Advanced Malware Protection can help protect against both unknown, zero-day threats and known malware, without impacting user productivity. Using a multi-layered approach, Trusteer Apex is designed to disrupt attacks at multiple “chokepoints” where the attacker has relatively few execution options. Some of its key capabilities for controlling these chokepoints—and breaking the attack chain—include:

- **Credential protection:** Trusteer Apex helps prevent users from submitting their credentials to harmful phishing sites; plus, it allows organizations to enforce password-reuse policies, resulting in less exposure from third-party site compromises.
- **Exploit chain disruption:** Trusteer Apex stops the exploit code from using known or unknown (zero-day) vulnerabilities to compromise an endpoint. The software protects commonly exploited and widely used applications that process untrusted external content, including browsers, Adobe Acrobat, Adobe Flash, Java and Microsoft Office.
- **Malware detection and mitigation:** Trusteer Apex can detect and remove known malware silently. This is particularly useful for detecting and mitigating massively distributed advanced persistent threats (APTs). Finally, cloud-based file inspection is also supported to help eliminate the noise of legacy threats.
- **Lockdown for Java:** Trusteer Apex can prevent malicious Java applications from executing high-risk actions, such as writing to the file system or making changes to the registry. Plus, it enables security teams to set the trust level for Java applications, reducing false positives and user disruptions.
- **Malicious communication prevention:** Trusteer Apex can stop malware from communicating with the Internet (for example, to a command-and-control server). It restricts processes from establishing external communications either by direct connection or abusing/tampering with other application processes.

In addition to exploit blocking, IBM Security Network Protection delivers advanced features, such as web application protection and application control. The all-in-one appliance platform provides integrated SSL inspection, real-time IP reputation analysis and continuous monitoring to help prevent active beaconing. And its advanced controls help block access to malicious websites and prevent web application misuse.
Putting it all together

Trusteer Apex and IBM Security Network Protection integrate with IBM Security QRadar® solutions to provide comprehensive security intelligence and incident forensics. Together, the solutions can disrupt malicious activity throughout the attack chain:

- **Break in:** When malware is delivered in a phishing email, IBM Security Network Protection prevents the exploit from reaching the vulnerable browser and alerts QRadar to the intrusion attempt.
- **Latch on:** When a remote employee opens an untrusted attachment, Trusteer Apex prevents the malware from installing, notifies QRadar and enforces a quarantine rule in IBM Security Network Protection.
- **Expand:** When attackers try to find privileged credentials, IBM Security Network Protection prevents the attempt to scan internal systems, while QRadar detects abnormal traffic on the network.
- **Gather:** When an internal system tries to export critical data, QRadar detects the user logins and database activity revealing abnormal access to sensitive servers.
- **Exfiltrate:** When abnormal, slow data transfers occur, QRadar detects the behavior, sends a quarantine rule to IBM Security Network Protection and records the attack activity.

---

**Multi-layered defense architecture**

**Threat and risk reporting**
Vulnerability mapping and critical event reporting

**Advanced threat analysis and turnkey service**

<table>
<thead>
<tr>
<th>Credential protection</th>
<th>Exploit chain disruption</th>
<th>Malware detection and mitigation</th>
<th>Lockdown for Java</th>
<th>Malicious communication prevention</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Prevent reuse on non-corporate sites</td>
<td>• Block anomalous activity caused by exploits</td>
<td>• Provide detection and mitigation of massively distributed APTs</td>
<td>• Block high-risk actions by malicious Java applications</td>
<td>• Block malware communication</td>
</tr>
<tr>
<td>• Protect against submission on phishing sites</td>
<td>• Gain zero-day defense by controlling exploit chain</td>
<td>• Apply cloud-based detection of known threats</td>
<td>• Administer the trust level reducing user disruption</td>
<td>• Disrupt command and control</td>
</tr>
<tr>
<td>• Report on credential usage</td>
<td></td>
<td>• Gain zero-day defense by controlling exploit chain</td>
<td></td>
<td>• Protect against data exfiltration</td>
</tr>
</tbody>
</table>

**Global threat research and intelligence**
Global threat intelligence delivered in near-real time from the cloud
Conclusion
In this era of nearly continuous security breaches, IBM can help thwart the most sophisticated attacks with proven, integrated solutions for behavior-based protection. These intelligent solutions empower organizations to detect malicious behavior across networks and endpoints in real time, so they can break the attack chain before any damage can occur. IBM takes protection beyond the limited effectiveness of point solutions and signature-based security with next-generation systems for intrusion prevention, malware protection and intelligent diagnostic forensics.

For more information
To learn more about IBM Security solutions for behavior-based protection, please contact your IBM representative or IBM Business Partner, or visit: ibm.com/security/threat-protection