THE IT TRIFECTA: Secure, Compliant, and Well-Managed

Modern enterprises are doing their best to address 3 simultaneous and closely interrelated objectives for their information technology infrastructure:

- **Demonstrate compliance** with policies and report progress against an initial baseline and targeted metrics.
- **Identify and assess** security-related risks, and manage them to an acceptable level.
- **Achieve and Sustain Compliance** ongoing.

ONGOING ONGOING FORWARD LOOKING

Detect, investigate, and respond to suspicious behaviors, security incidents and breaches.

Manage Security-Related Risks

Improve the efficiency and cost-effectiveness of ongoing operations.

Reduce the total annual cost of operations and optimize efficiency of day-to-day management.

Optimize Ongoing Operations

Looking forward, the most valuable security analysts and operational staff will be those who can successfully interpret the implications of the intelligence generated from security monitoring and analytics platforms — not only for staying secure and compliant, but also to proactively drive the infrastructure optimizations that contribute to achieving the strategic objectives of the business.

A platform approach helps enterprises to achieve:

- Better analytics, to help operational staff prioritize and take faster action on the most relevant information.
- Better integration of actionable intelligence, to optimize and target responses.
- Better visibility into a rapidly changing threat landscape, and an increasingly complex computing infrastructure.

SAVING TIME AND MONEY: The Business Benefits of Platforms

Companies that leverage a security monitoring and analytics platform have a faster detection response time and a reduced business impact on attacks in both availability and confidentiality.

<table>
<thead>
<tr>
<th>ATTACKS ON AVAILABILITY</th>
<th>2X 70%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time for Detection &amp; Response</td>
<td>Immediate response = 100% reduction in business impact</td>
</tr>
<tr>
<td>Attack on Time to Detection &amp; Response</td>
<td>Reduction in Business Impact</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ATTACKS ON CONFIDENTIALITY</th>
<th>2X 30%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time for Detection &amp; Response</td>
<td>50% time reduction</td>
</tr>
<tr>
<td>Attack on Time to Detection &amp; Response</td>
<td>30% business impact reduction</td>
</tr>
</tbody>
</table>

Companies commonly get started on their security monitoring and analytics initiatives with tools that help with forensic investigations, after-the-fact auditing, and reporting on compliance and work progress.