Where Technology Means More®

5 Ways to SOAR Beyond a Critical Skills Gap

By: **ePlus Security Team**

The cloud is big, with 94% of enterprises using it to augment existing capabilities. And the cloud is pervasive, with industry experts estimating that 83% of workloads will run in these environments by 2020.[1]

Yet, the cloud is also vulnerable. For as a recent survey of 300 senior executives reported, 52% of multi-cloud and 24% of hybrid-cloud environments have suffered security breaches during 2018 and 2019.[2]

Attacks happen because the cloud is hard to protect. These heterogeneous environments suffer from a perfect storm of vulnerabilities: significant staffing and resource shortages, security skills gaps, and between 40 and 50 costly security tools that are being underutilized and underleveraged.

Many overstretched IT departments are responding with SOAR. Security Orchestration, Automation, and Response combines a number of security technologies into a single pane of glass for addressing vulnerabilities more efficiently and effectively.

In my experience, organizations that make the switch derive 5 important benefits from changing how they handle infrastructure threats.

[1] "Cloud Adoption Statistics for 2019." HostingTribunal.com. 2019.

[2] Peter Suclu. "Multi-Cloud Strategy May Pose Higher Security Risk: Study." TechNewsWorld Cybersecurity. September 6, 2019.

e+ Where Technology Means More®

1. Improve MTTD and MTTR

Cloud environments are complex because they contain thousands of assets. These components – plus, even more mobile and Internet of Things devices – are contributing to a huge expansion of the traditional attack surface. The results in networks that are hard to manage, monitor, and control.

When SOAR is implemented as part of a platform solution, organizations are able to reduce the attack surface by aggregating asset data, behaviors, and threats into branched workflows. These workflows allow security analysts and engineers to automate the incidence-response process and resolve possible attacks so human operators can exercise control without being overwhelmed by false alerts.

SOAR also correlates siloed data into reports, analyses, and actions that reduce the need for manual processes. These efficiencies help security operations centers (SOCs) to improve mean time to detect (MTTD) and mean time to respond (MTTR). Optimizing MTTD and MTTR enables SOCs to combat sophisticated threats wherever they occur in the technology stack.

2. Reduce complexity

Many organizations are spending scarce funds on poorly utilized technologies. They are pursuing security piecemeal and ending up with more data silos, visibility gaps, and so many alerts that they are overwhelming security personnel and slowing response times. And their overwhelmed staff are making mistakes. As Gartner recently reported, these failures are causing errors and introducing more problems into already chaotic environments.[3]

SOAR helps to reduce this complexity by providing a framework for orchestrating existing automation tools into individual workflows. Organizations are able to optimize tools, which enhances their defenses by allowing them to know exactly what they have in place, how it is being used, and how they can leverage technology to improve security.

SOAR makes it easier to create usage policies and scripts for enforcing safe choices, managing resource consumption, and controlling the ability of users to change infrastructure or provision new systems or assets. Organizations are able to rationalize the wide range of toolsets they have in place across environments. These changes lead to efficiencies in tool usage and allow staff to react to threats with more timely and effective responses.

[3] Stan Black. "The View from the Gartner Security & Risk Management Summit: Beyond Traditional Models and Vendors." Citrix.com. July 24,2017.

3. Optimize the talent pool

IT teams are suffering from a shortage of qualified staff even as the threat of attack is growing. As a recent survey confirmed, most organizations are understaffed because good cybersecurity talent is hard to find. Among respondents, 73 % agreed they needed more staff and 70 % said they could not retain and recruit qualified staff.[4]

SOAR helps by reducing the burden on current staff. By funneling threats into efficient workflows, it improves efficiency by better prioritizing threats and vulnerabilities. This measure allows smaller teams to improve security results. It also creates bandwidth for training staff for specialized security roles and expanding practical competencies as the threat landscape continues to evolve.

[4] "Staffing the IT Security Function in the Age of Automation: A Study of Organizations in the United States, United Kingdom, and APAC." Ponemon Institute. 2019.

4. Accelerate threat containment and remediation

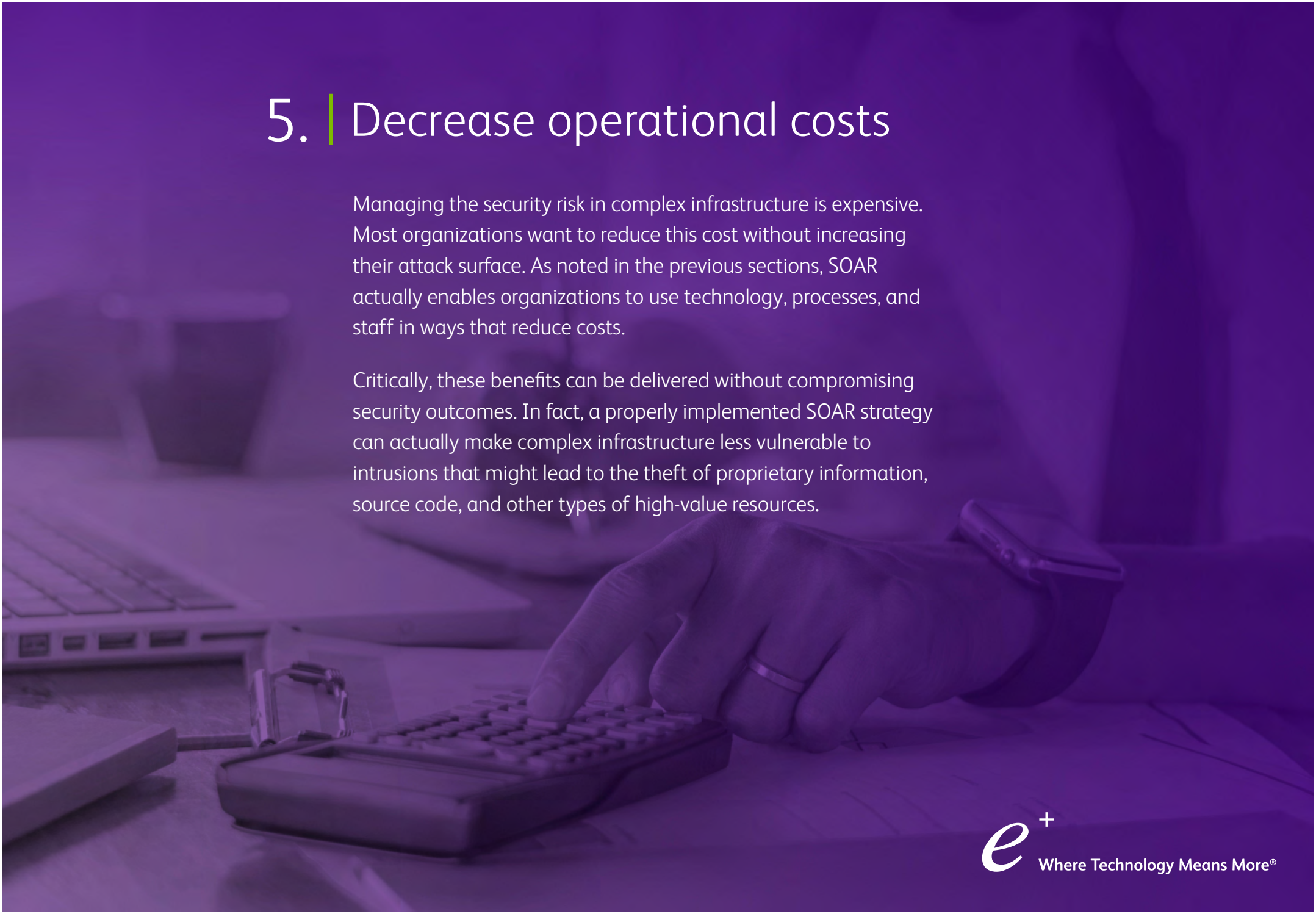
Many security tasks are managed by security professionals. These workers often must review and respond to hundreds, thousands, or tens of thousands of alerts each week. Such workloads create alert fatigue and leave little time for documenting incidents, catching visibility gaps, or updating processes to reduce existing attack surfaces.

SOAR tools address these challenges by automating incident response across the environment. Consolidating data from multiple threat feeds, scanning tools, logs, and systems improves efficiency by eliminating manual tasks. Delivering all this information to a single pane of glass or a few simple dashboards helps staff make good decisions more quickly. It also creates a full audit trail for post-event reviews and compliance and governance reporting.

5. Decrease operational costs

Managing the security risk in complex infrastructure is expensive. Most organizations want to reduce this cost without increasing their attack surface. As noted in the previous sections, SOAR actually enables organizations to use technology, processes, and staff in ways that reduce costs.

Critically, these benefits can be delivered without compromising security outcomes. In fact, a properly implemented SOAR strategy can actually make complex infrastructure less vulnerable to intrusions that might lead to the theft of proprietary information, source code, and other types of high-value resources.



Where Technology
Means More®

eplus-security@eplus.com

www.eplus.com/security

ePlus Technology | 13595 Dulles Technology Drive | Herndon, VA 20171