NETCITADEL
INTELLIGENT NETWORK SECURITY™

A NetCitadel White Paper

Security Orchestration:

Why Today's IT Agility Initiatives Will Fail Without It!

Security Orchestration:
Why Today’s Dynamic Enterprises Require a New Paradigm for Network Security

Executive Summary

Today’s enterprises are being held back by legacy security infrastructure that requires a steady stream of manual updates to maintain effective protection in the face of constant changes to their computing environments. This situation is only becoming more acute as firewalls and other traditional security devices have also begun to impede investments being made in virtualization, cloud computing, and other technologies intended to enhance IT agility.

Introducing a new paradigm, Security Orchestration solves this mounting problem by transforming existing, static security products into dynamic defenses capable of automatically adapting to changing conditions. Resulting benefits include reduced operational and capital expenditures, tighter and more effective network protection, and the removal of security as a significant obstacle in the path to maximizing IT agility.

The Only Constant Is Change

Embracing change has always been an important part of maintaining relevance to one’s customers and an edge over the competition. Over the past decade, however, there has been an unprecedented increase in both the volume and speed of changes required by IT to “meet the needs of the business.”

To begin with, today’s IT and information security teams must account for:

- **More applications** – as new business services and resources are brought online faster than old ones are retired.
- **More users** – as the business extends access and services to a growing number of contractors, partners, and customers.
- **More devices** – as the proliferation of mobile form factors continues to progress.
- **More threats** – as malware and other types of attacks not only become increasingly prevalent but also increase the need for real-time responses.
- **More defenses** – as the so-called “dissolving perimeter” drives the need to deploy countermeasures more pervasively throughout an organization’s network.

This base level of change common to all enterprises is nothing, though, compared to what is now being encountered by organizations attempting to maximize IT agility by deploying virtualization technologies and adopting cloud computing to transform their once static networks and systems into highly dynamic computing environments.

The impact, in this case, is not only an order-of-magnitude increase in the number of changes that IT security must accommodate – driven in part by how trivial the task of deploying new applications has become – but also the speed with which these changes must be made. Historically, when new applications and servers were introduced, IT Security had days, weeks or even months to plan and execute the changes needed to ensure an adequate level of protection and compliance was maintained. But with highly dynamic computing environments, these changes need to be made in real-time.

The Network Security Bottleneck

Whether it's the need to handle considerably more IT changes as a matter of routine, the need to respond more quickly than ever before due to increasing investments in dynamic infrastructure, or both, the real challenge facing today's organizations is the inability of their network security infrastructure to keep up.

The net result is that legacy, static security infrastructure is an impediment to implementing routine, business-driven changes within IT. From a strategic perspective, it is also keeping today's enterprises from fully realizing the benefits of the investments being made to build highly dynamic computing environments.

Better planning and more efficient processes can only take the security team so far. Beyond that, it's up to the technology that has been deployed – in this case, the firewalls, routers, and other network security devices capable of controlling which resources are accessible to which users and systems.

Unfortunately, the waves of innovation spreading across other areas of IT over the past decade have had little influence on network security devices. Speeds and feeds have increased, and complementary countermeasures such as network anti-virus and intrusion prevention have become co-resident to enable device consolidation and reduce network complexity. But even with the relatively recent introduction of next-generation firewalls, the only significant change has been the ability to more granularly control who is granted access (i.e., user identity) and what it is they have access to (i.e., application identity).

The bottom line is that no meaningful improvements have been made to rectify the fact today's network security devices are essentially blind. They rely on a decades-old foundation of static policies and have no visibility into or understanding of the evolved computing environment in which they are deployed. Consequently, they are unable to adjust the protection being provided based on changing conditions. Re-configuring them so that they continue to deliver adequate protection remains a manual, error-prone, and time-consuming exercise.

The net result is that legacy, static security infrastructure is an impediment to implementing routine, business-driven changes within IT. From a strategic perspective, it is also keeping today's enterprises from fully realizing the benefits of the investments being made to build highly dynamic computing environments.

Security Orchestration – A New Paradigm for Enterprise Security

Today's organizations need a better way to manage their security infrastructure to have it keep up with the speed of business. The answer to this problem is Security Orchestration.

The objective with Security Orchestration is to make otherwise static security infrastructure dynamic in such a way that it becomes adaptive to changing conditions – without having to alter any base-level policies. At a high level this is accomplished by bridging the gap between enterprise security devices and the information they require in order to provide effective security.

As daunting as such a solution might sound, it is important to recognize that although Security Orchestration represents a new paradigm for enterprise security, it is actually based on a proven approach. The same general technique – having an external management system monitor relevant system parameters and subsequently use this information as the basis to provision, de-provision, migrate, or otherwise adjust virtual machines – is what lies at the heart of leading server virtualization solutions. It's also the approach being employed by emerging solutions for Software Defined Networking.

Having the ability to sequentially update a series of devices is not enough. Scalability by design accounts for the proliferation of IT changes and closes security gaps in real-time by enabling thousands of updates to be pushed out simultaneously.

Transforming Static Security Infrastructure into Intelligent, Adaptive Defenses

With Security Orchestration, the "external management system" is an intelligent control plane for security. Similar in concept to a Network Controller for Software Defined Networking, this core component works at a high level by:

- Maintaining connections with key elements of the computing environment – including physical, virtual, and cloud infrastructure management systems – to enable real-time detection of changing conditions.
- Maintaining connections with other sources of intelligence that are ultimately relevant to maintaining robust defenses, such as directories, identity, and threat management systems, and custom-developed information stores.
- Coordinating and intelligently mapping the contextual information it gathers to an organization's security infrastructure, including physical firewalls, virtual firewalls, cloud security services, routers, and other devices capable of enforcing access control rules and other essential security policies.

Because the data collection and mapping are fully automated, the net result is the transformation of otherwise blind and static security devices into dynamic defenses capable of responding to changing conditions in near real-time.

Critical Characteristics and Capabilities

Security Orchestration promises not only to facilitate routine changes to an organization's IT infrastructure, but also to accelerate the transformation to virtualized data centers and the adoption of highly agile cloud computing solutions. Fully realizing this potential, however, depends on more than just the high level ability to gather a broad spectrum of intelligence and use it to dynamically re-configure an organization's security devices. Other key elements and capabilities of an enterprise-class Security Orchestration solution include the following solutions.

A unified policy framework. A unified and simplified policy model is one of the keys not only to supporting today's heterogeneous networks – by including coverage for multiple brands/versions of firewalls and types of policy enforcement devices – but also to having a seamlessly extensible solution. Without it, the solution will fail to provide sufficient coverage and become unmanageable as each new device requires its own unique policy model and management interface. Operational efficiency and usability are also improved by replacing nebulous networking attributes (e.g., ports, protocols, and addresses) with commonly understood business language (e.g., the names of applications and user groups).

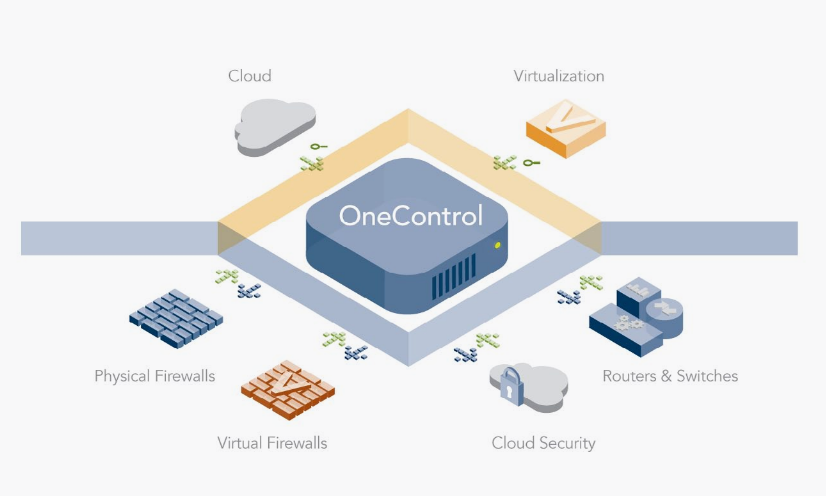

Figure 1 Deployed as a virtual appliance, OneControl conveniently supports two modes of operation

Flexible adoption/implementation. Organizations will adopt Security Orchestration solutions at different paces, so a comprehensive solution needs to be able to flexibly support multiple deployment modes. The two most common deployment modes are mapping-only and full policy. Mapping-only deployment mode provides a lightweight way to introduce Security Orchestration into an environment by minimizing device updates to only include abstract objects on the security devices, not the firewall rules themselves. Organizations that are farther along in their adoption of Security Orchestration require support for full policy mode, where security updates include firewall rule changes.

Embedded business logic. Complete Security Orchestration solutions need to include the ability to flexibly define business logic rules establishing the relationships between infrastructure elements and the security devices protecting them. Without this business logic definition the Security Orchestration solution will not know which security devices to update when a change in the network is detected.

Scalability by design. Having the ability to sequentially update a series of devices is not enough. Scalability by design accounts for the proliferation of IT changes and closes security gaps in real-time by enabling thousands of updates to be pushed out simultaneously.

Restoring Security Effectiveness While Enabling IT and Business Transformation

The bottom line is that the process of maintaining effective security is becoming an increasingly significant bottleneck to today's businesses, whether it's standing in the way of incremental progress such as the addition of a new application, or more strategic initiatives such as the transformation to a highly dynamic and agile computing environment. To rectify this situation, Security Orchestration introduces a new paradigm for enterprise security – one that leverages proven techniques to transform static security devices into dynamic defenses that are aware of the environment they are protecting and, therefore, capable of automatically adapting to changing conditions.

Specific, tactical and operational benefits of an enterprise Security Orchestration solution as described in this paper include the following features:

- Affordability and ease of implementation – as the solution works with existing infrastructure, avoiding the need for upgrades and the need to abandon existing hardware investments.
- Efficient operations – as a centralized rather than siloed security model reduces management effort and helps ensure consistent policy enforcement.
- Broad/comprehensive coverage – as support for multi-vendor on-premise, virtual, and cloud-based infrastructure avoids the need to implement multiple overlapping solutions.

Additional Strategic and Business-Oriented Benefits Include:

- Increased IT and business agility – as Security Orchestration facilitates routine changes to IT infrastructure and accelerates the transformation to a highly dynamic computing environment.
- Reduced operating expenditures – as intelligent automation cuts the time and effort required to administer security infrastructure despite the proliferation of required configuration changes.
- Reduced capital expenditures – as the infusion of additional intelligence and advanced capabilities extends security infrastructure refresh cycles.
- Reduced risk – as IT gains the ability to accommodate rapid-fire IT changes without having to compromise in terms of access control and other defenses.
- Improved compliance posture – as the solution provides the opportunity to automatically track security-related configuration changes and tie them to associated business justification.

About NetCitadel

Founded by industry veterans with decades of cumulative experience developing security automation solutions for large-scale environments, NetCitadel is uniquely positioned as an innovator and pioneer in Security Orchestration. Our flagship solution, OneControl Security Orchestration Platform, transforms existing static security devices spanning physical, virtual, and cloud environments into a dynamic defensive infrastructure capable of automatically adapting to changing conditions in real-time. With OneControl Security Orchestration Platform, today's enterprises obtain an automation solution that dramatically simplifies the never-ending task of maintaining effective security and removes it as an obstacle to realizing the full potential of virtualized data centers, cloud computing, and other investments made to maximize IT and business agility.

www.netcitadel.com
2513 E. Charleston Rd. Suite 100
Mountain View, CA 94043
Phone: (650) 564-4285