

# BECOME A SERVICE-AWARE ENTERPRISE

Understanding complex and changing boundaries reduces risk and increases security awareness.



**BOB OSBORN**  
CHIEF TECHNOLOGY  
OFFICER FOR FEDERAL,  
SERVICENOW

**THE DAYS OF THE** “Fortress Enterprise,” with clearly defined and protected edges to the computing environment, are over. As agencies update their cybersecurity strategy, the new normal of constant expansion and contraction of the computing edge must be taken into account.

For decades, we have designed and implemented IT architectures with this image of defending a fortress. Clean edges, technologies, and carefully measured purpose vs. risk are all known, planned and purpose built. Almost as an afterthought, we would put in process controls to limit any changes. Once complete, the architecture became a reference document instead of an operating model.

With the adoption of the cloud and with agencies expanding the computing boundary into commercial data centers, that approach is no longer valid. Furthermore, with the advent of the Internet of Things (IoT) and the seemingly limitless potential for new devices connecting to our networks, we must be more contextually aware of the entire enterprise computing boundaries in real-time and adapt to a new holistic security service delivery model.

As we receive more data from IoT devices, we need a fully service-aware capability to understand the state of our computing environment and maintain a contextual understanding of risk. Employing platform-based modern applications that leverage a service-aware configuration management database (CMDB), platform automation and artificial intelligence (AI) can help agencies achieve real-time visibility, contextual awareness and their risk status. New technologies will enhance this coordinated and contextually aware approach to traditional network and security operations.

## Automation and Artificial Intelligence

As fast as threats are developed and new technologies are created to mitigate those

threats, the ability of agencies to acquire new computing capabilities are limited by traditional protocols. It is advisable to leverage a modern platform that delivers state of the art applications over an enterprise class cloud via a subscription acquisition model. That way agencies can finally keep up with current technology developments. Agencies have had to understand what technologies were available, then acquire and integrate that technology. Using a subscription-based model to acquire new software changes the game.

Agencies can modernize their environment to become service-aware. At its most mature end, this service-aware enterprise is driven by AI and machine learning. Having these game-changing technologies helps agencies understand and manage IoT. Alerts from the platform bring human decision-making into the event at the appropriate time with the information needed for a human decision.

Another critical cybersecurity component is the architectural approach to identity management and access control. Simply put, agencies must identify who is requesting access with what device and control their ability to interact with agency databases. Any issue with access control opens the door for bad guys to penetrate our defenses, infiltrate databases and steal information.

The service-aware enterprise must recognize the device, its location and its owner's authority to access various data from our computing environment. This must be done in milliseconds and with near zero error rate, which automation and AI make possible. These elements working together in harmony creates the type of “living” service-aware enterprise necessary to operate securely in today's world.

*Bob Osborn is chief technology officer for federal at ServiceNow.*

# GET YOUR SECURITY IN CHECK

---

PROTECT:



DETECT:



RESPOND:



Without rapid threat response,  
your security is incomplete

**A serious threat has been detected—now what?**

Frantic emails. Missed phone calls. Time-consuming manual processes. Without intelligent remediation tools, your security is incomplete. ServiceNow brings data from existing tools into a structured response engine that runs on the same platform as IT. Now alerts are automatically prioritized and you can solve real threats—fast.

[www.carahsoft.com/innovation/servicenow-cybersecurity](http://www.carahsoft.com/innovation/servicenow-cybersecurity)

[servicenow.com](http://servicenow.com)

servicenow<sup>®</sup>