THE SELF-SUSTAINING ENTERPRISE

USING TECHNOLOGY INNOVATION TO ENHANCE CYBERSECURITY SKILLS
THE SELF-SUSTAINING ENTERPRISE

Businesses operate in a digital ecosystem that is becoming ever more connected, collaborative and complex.

One way to think about this is in the context of your own neighborhood. How do you understand and navigate your relationships? Some neighbors you know well, others are strangers. Visitors, deliveries, workers, commuters all come and go, creating an environment where you must be aware of the different risks that each visitor poses. Who can you trust? This is the precise question that businesses need to answer as the population of their own neighborhood—the digital ecosystem—dynamically changes and grows.

To navigate ecosystem relationships, it is important for companies to know their business processes well. They need to understand what is valuable to the business and the required operational resilience or, using the neighborhood analogy: “What’s in our house and how well have we protected or fortified our key assets?” As new challenges or opportunities arise, companies may choose to make selected processes more resilient while maintaining or optimally decreasing the level of risk.
As the risks within the ecosystem change, the infrastructure will need the agility to shift security postures in response. If a stranger shows up in your neighborhood, how do you respond? Do you question the stranger to establish who they are? Do you turn out the lights and pretend you are not at home? Or do you move your valuables to a hidden location?

Similarly, an organization will need to develop an ability to rapidly address and assimilate strangers—both people and devices—into the business ecosystem. It will also need new agility to sense and respond to threats and vulnerabilities as they present themselves. These are the characteristics of what we call “the self-sustaining enterprise.”

In such a complex, rapidly changing environment, being self-sustaining is only made possible if decisions are made at machine speed. Machines provide the predictive analytics and cognitive modeling that automate how enterprise security “thinks” about threats or risks. Infrastructure paradigms, such as network functions virtualization (NFV), software-defined networking and serverless architectures, introduce the agility needed to address those risks.

Advanced technologies make it possible for the enterprise to “think” and “react” more like a living organism, enabling it to adapt and realign to business goals and priorities as they evolve. It is all about continually finding new answers to the question: “How quickly can we recognize and adapt our services to the needs of our customers or business partners and protect ourselves from the next adversary?”
The deep symbiosis between people and technology creates new and heightened security risks. As the connectedness of physical and digital worlds increases, so does the attack surface.

PROLIFERATION OF INSECURE DEVICES CREATES AN EXPANDING ENTERPRISE ATTACK SURFACE

The attack surface for all organizations is expanding exponentially. By 2020 Cisco estimates that there will be in the region of 50 billion connected devices online, from thermostats, cars, locks and fitness monitors to manufacturing equipment, supply chain infrastructures, aircraft, power grids and public transport. Everything that can be connected, will be.

This proliferation of connected devices is taking place with little guidance or standards. Efforts to embed security measures have been largely left to the manufacturers and they, as yet, have no real incentive, economic or otherwise, to do so. The imperative to be first to market and maximize ease of use eclipses all other considerations. Even in the critical area of medical devices, the Food and Drug Administration has only just issued recommendations (December 2016) for medical manufacturers to provide post-market risk management—emphasizing that manufacturers should monitor, identify, and address cybersecurity vulnerabilities as part of their post-market management of medical devices.

MERGING OF PERSONAL AND PROFESSIONAL LIVES AND DATA EXTENDS THE ATTACK SURFACE

The trend to “bring your own device” will only gain momentum as people expand their personal connectedness with the many devices they bond with or are indentured to. The business is also increasingly stretching traditional enterprise boundaries through the distributed, liquid workforce where workers operate in different places and contexts (many of them lying beyond a business’s traditionally highly patrolled perimeter). As services extend to these workers, interactions and disruptions can be expected from other devices in their ecosystem: smart home devices are just one example. Collectively, these developments create a multidimensional surface for interaction, communications, and attack and/or exploitation.
THE FIRST FLURRIES BEFORE THE STORM?

The malware known as “Mirai” was responsible for the massive distributed denial-of-service (DDoS) attack on Dyn’s domain name system in October 2016 (in which reported attack rates were as high as 1.2 Tbps²). This impeded access to a range of some of the Internet’s biggest names in parts of the United States.

Mirai takes advantage of vulnerabilities in Internet of Things (IoT) connected devices, continuously scanning for ones that are protected only by factory default or hard-coded usernames/passwords.³ And it is worth noting that far from being a one-off attack, Mirai’s source code has been posted online, making it available to an army of new attackers. It is mutating faster than you can read these words and, in view of these developments, it is perhaps no coincidence that Mirai means “future” in Japanese.

EXPANDING ATTACK SURFACES EXPLOITED BY ATTACKERS: THE WEAPONIZATION OF THE INTERNET

So how are well-funded and sophisticated attackers exploiting this fertile terrain? The stark truth: they are turning apparently benign devices into weapons capable of causing massive harm to corporations, industries, and even nation states.

In a connected digital world, the risk resides both in the devices themselves, and in the cloud services to which they send their data. In a worst-case scenario, compromising those cloud services could cede to an attacker centralized command and control over a huge number of devices.

The scale and frequency of the attacks we are seeing today are likely just the first flurries before the storm (see above). Cyber-attacks taking advantage of the proliferation of unsecured devices (not to mention the growing ecosystem of identities, applications, data and networks) are growing in sophistication and reach every day. And as this happens, the onus is on organizations to develop a very different mind-set and approach to security—one in which trust becomes critical.
UNDERSTANDING TRUST IN THE NEW BUSINESS ECOSYSTEM

In a self-sustaining enterprise, it is imperative to know what is important for the business to function to take the appropriate actions regarding the level of security and protection that specific assets require.

Today, this assessment relies on human-intensive and error-prone data collection, with employees having to attest to what devices or assets are, and how they are used. As it describes just one moment in time, this data must be constantly updated to keep pace with changes in the business and how it functions.

In the new business ecosystem, organizations will need capabilities that discover and analytically classify the role of an asset in a continuous manner. Once understood, the business will need to agree and establish an acceptable risk which then informs the level of trust required for every asset—user, device and data element. Organizations will shape security controls based on the degree of trust for assets, and deploy trust-based authentication mechanisms that assign each device a “trust level” that guides the requirements needed for access.

Similarly, each business process needs to be understood in terms of the technical infrastructure—the neighborhood of assets that work together to implement it. The process’s business value and sensitivity will drive the requirements for control and protection, defining the risk level of the neighborhood. Processes with similar requirements could be aggregated into these neighborhoods which can then be uniformly managed with a common set of controls and protections—an adaptive, intelligent security platform—to streamline security operations and reduce complexity.
A FRAMEWORK FOR MEASURING TRUST LEVELS: KEY CONSIDERATIONS

AN ASSET’S TRUST LEVEL CAN BE COMPUTED BY COMBINING SEVERAL FACTORS:

The identity that it proclaims through attestation

The degree of control an enterprise has over the device (including corporate, third-party, personal and smart building/infrastructure)

Factors that help to measure trust such as:

• Exposure to unknown devices (if an unknown device is added to a neighborhood, it may be used to attack other devices, reducing trust temporarily)

• Exposure of the device to vulnerabilities: is it something the enterprise can patch? If not, the device needs to be categorized with a lower degree of trust.
CHARACTERISTICS OF ADAPTIVE, INTELLIGENT SECURITY PLATFORMS

Enterprise security needs to leverage Artificial Intelligence (AI) and new infrastructure paradigms to keep pace with changing attack surfaces.

This means having:

• an operating model that provides an in-depth understanding of the risk from devices and vulnerabilities within the environment, their potential impact on business processes, along with the agility to mitigate identified risks quickly
• a persistent identity and the capability to analytically identify assets and their role and function
• security embedded into how the enterprise works, transparently guiding the business to behave securely
• the flexibility needed to dynamically segment and enforce behaviors and policy throughout the infrastructure.

So what actions can organizations take to achieve a self-sustaining security platform?

BE ANALYTICAL ABOUT IDENTITY

In practice, identity is largely dependent on knowledge, membership or relationships. Roles and functions are defined based on the repository of knowledge. The self-sustaining enterprise will require more sophisticated identity methods to keep pace with the ability to manage persistent identity.

Persistent identity, assurance that actions are indeed the authorized user’s and not someone using a phished account, are fundamental to the model. There are now many persistent identity solutions, including DARPA’s Active Authentication behavioral biometrics challenge—based on unobservable human biometrics. The “RUU” solution by Accenture Labs and Allure Security Technology demonstrated high fidelity through a small client footprint.
Identity and Access Management (IAM) services must also keep up with the speed of business. IAM value realization is often impeded by too many choke points. As the number of applications and systems grow, the manual workforce and corresponding effort grows with it, leading to a less effective and more error prone process. To realize the value of IAM investments, leading organizations are moving to Robotics Process Automation (RPA) to orchestrate the very structured and repetitive tasks. RPA closes the efficiency gap that is created by an antiquated reliance on manual processes. Accenture is bringing robotics to life by connecting isolated applications in a holistic automation capability.

In a serverless architecture, applications are deconstructed into microservices that run and auto-scale dynamically. This lowers cost to the business and enables a rapid development cycle. Huge applications with static code and container-based applications are replaced with individual functions that are only run on demand. Certain common functions, like authentication, are provided, updated and maintained by the vendor. Businesses must continue to write secure code, but they can leave the deployment and running of the functions to the trusted vendor. Providers like Amazon Web Services, Lambda or Apache OpenWhisk, motivated to provide high quality services, manage the underlying security of the servers and the data.

Moving applications to a serverless model requires a high level of operational maturity. The business must be able to deconstruct applications into microservices and events and be clear on access controls, data protection and expected behaviors. Additionally, the business must define the data needs and choreography of the events and communications (the data flow between each function). Once the expected choreography and behaviors have been articulated, the enterprise can focus on behavior: leveraging artificial intelligence to monitor, model and learn granular application behavior. The behavioral fingerprint will enable it to identify and even anticipate potential threats to the business.

CONSIDER SERVERLESS

Leading businesses are looking closely at the serverless opportunity. Grown from cloud thinking, serverless is a more far-reaching computing approach that changes how the business creates and manages applications.

Serverless refers to a new paradigm of building applications where the business focuses more on its business application functions and less on the processing and hardware needed to run these functions. The operational aspects of managing applications, such as maintaining servers, scaling and deploying are managed by a third-party vendor.
Think about infrastructure and security as code

For infrastructure that remains in the enterprise, controls should be designed independently of the physical infrastructure. By abstracting security in this way, the business can leverage virtualization to efficiently deliver the required security to assets. Software-defined security provides the flexibility and agility needed to control and quarantine small parts of the network/device, taking advantage of micro-segmentation and enabling the self-sustaining enterprise. In combination with an orchestration engine like Service Now, businesses can be responsive to changing risk conditions, with the ability to move in and out of environments, while ensuring a consistent level of security control is in place. More specialized security orchestration can be delivered through solutions like Phantom, that create a foundation on which to layer cognitive modeling to enhance security decisions.

With a software-defined security approach, an asset can attest to its role and function within the enterprise, orchestrated security services validate that attestation and assign a degree of trust, and security functions are delivered and calibrated to the asset’s role and perceived risks. This automatic ability to continuously shape the security environment is, in large part, what enables the self-sustaining enterprise.

Be dynamic—segment, move, shapeshift

Think again about the neighborhood: in a heavily virtualized environment an organization would be able to dynamically provision access to the neighborhood, as well as dynamically assign new housing to it. As new compute assets become available, the organization could rapidly engage with the assets that best support its business functions. Business processes with similar risk could be grouped into subdivisions to better enforce controls and behavior, enabling more effective management of risks.

As threats or risks change, the self-sustaining enterprise would use this same approach to dynamically segment network traffic or resources to manage business risk or contain an incident. Tempered Networks has moved forward with a solution that takes advantage of orchestration to enable fast provisioning and de-provisioning of networks. With security in mind, it leverages this to instantly segment, protect, cloak, failover or revoke any device or resource on the network. Dynamic segmentation and micro-segmentation capabilities enable the security organization to respond to threats, adapting protections to maintain the agreed-upon risk posture with the business.

Another dynamic technique to manage threats and vulnerabilities is to shapeshift or morph, making the target invisible or continuously incomprehensible to the attacker. For high business value assets or services, a polymorphic approach could be used (see page 13).
**POLYMORPHIC MODELS EXPLAINED**

In a “polymorphic model”, resources and technologies dynamically evolve based on a developing understanding of both the threats to which they may be vulnerable and the degree to which they may be trusted. Where needed, additional polymorphic controls can be layered onto high-risk devices to make the attack surface even more dynamic, protecting it from targeted attacks. In our model definition, serverless and software-defined networking, when applied dynamically to actively manage risk under changing conditions, could be considered elements of a polymorphic security model.

In these models, it is possible to change—morph—the targeted assets to reduce the effectiveness of an attack, or eliminate the viability of any critical vulnerability. Morphisec® uses a polymorphic approach to protect applications as they process in-memory. As an application, Web browser or OS loads to the memory space, a polymorphic engine scrambles the inner structure of the process, its calls to library functions and library addresses, making the memory unpredictable to attackers.

As business ecosystems continue to extend and intermesh, business assets will be exposed to new threats. To effectively manage these risks, organizations need an operating model that leverages all the capabilities described. Together, these enable the self-sustaining enterprise to rapidly identify devices, understand the threats that they pose to the organization, and shift the security posture of the organization to quickly mitigate the impact of any vulnerability or exposure.
Successful businesses will enable connectivity and collaboration through self-sustaining practices. To operate at digital speed and with agility, security must move at the same machine speeds. With a self-sustaining approach, existing cybersecurity capabilities are enhanced through automation, machine learning, software-defined networking and new approaches to infrastructure to maximize resilience and support swift recovery from any disruption.

In doing so, organizations can be safe in their neighborhood. They can know who is in the neighborhood and collaborate when and where it makes sense. And, the best part, they have the agility to change—to meet new business opportunities and safely navigate when conditions are unfavorable or threats arise.
GETTING STARTED: LAYING THE GROUNDWORK FOR BUILDING A SELF-SUSTAINING ENTERPRISE

Understand the availability and sustainability goals for key business processes based on an acceptable level of risk to the organization.

Identify the applications that could be logically separated from their operational components into microservices and events.

Consider how these security services could be shared for reuse and consistency. Evaluate how they could be more effectively applied to the microservices and events. Revisit the security requirements for business functions and services.

Identify security functions that can be provided as a virtual service through serverless and network virtualized functions of software-defined networking.

Build a robust identity and access management system that can detect and manage both new and existing assets—including users, devices, data and communications—to dynamically and continuously determine how trusted they are.

Integrate products and/or techniques that will “think” and “react” with minimal human effort—like artificial intelligence and advanced analytics—to enable the self-sustaining environment.
CONTRIBUTORS

Marc Carrel-Billiard
Global Managing Director
Accenture Technology R&D
marc.carrel-billiard@accenture.com

Lisa O’Connor
Managing Director
Accenture Labs, Security R&D
lisa.oconnor@accenture.com

Matt Carver
Senior Manager
Accenture Labs, Security R&D
matthew.carver@accenture.com

Malek Ben Salem
Senior Principal
Accenture Labs, Security R&D
malek.b.salem@accenture.com

Robin Burkett
Senior Analyst
Accenture Labs, Security R&D
robin.l.burkett@accenture.com

REFERENCES

7. https://www.phantom.us/
ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions – underpinned by the world’s largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 401,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

ABOUT ACCENTURE LABS

Accenture Labs incubates and prototypes new concepts through applied R&D projects that are expected to have a significant strategic impact on clients’ businesses. Our dedicated team of technologists and researchers work with leaders across the company to invest in, incubate and deliver breakthrough ideas and solutions that help our clients create new sources of business advantage.

Accenture Labs is located in seven key research hubs around the world: Silicon Valley, CA; Sophia Antipolis, France; Arlington, Virginia; Beijing, China; Bangalore, India; Herzliya, Israel and Dublin, Ireland. The Labs collaborates extensively with Accenture’s network of nearly 400 innovation centers, studios and centers of excellence located in 92 cities and 35 countries globally to deliver cutting-edge research, insights and solutions to clients where they operate and live. For more information, please visit www.accenture.com/labs.

This document makes descriptive reference to trademarks that may be owned by others. The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks.