
# Bringing Effective Security Into Focus

cisco

# Digitization in a world of complexity

## Inside your business, we know it's all about innovation to create digital business transformation.

At the network edge, where your apps meet the road and where new IoT devices will drive fundamental business change, consistent connectivity and strong networks keep users for good, improve device performance and drive the insights needed to stay competitive.

The pursuit of effective security is unlike the pursuit of effective IT, where outcomes can be measured by tangible results such as greater uptime and connectivity, costs savings or more productivity and performance. Security is effective when nothing happens: no data breaches, no Distributed Denials of Service (DDOS) attacks and no ransomware.

Achieving this zen-like state in the ever-complex and changing IT infrastructure like trying to get out of never-ending labyrinth of increasing complexity.

Today's security leaders are tasked with protecting an attack surface that has never been more diverse or more complex. Let's look at the elements of complexity we have to deal with today.

### Frankenstructures

Today's IT landscape is a complicated one – one that has become a cobbled together "frankenstructure". And we are being asked to use this to spark digital digital business transformation. But that is close to impossible with networks that are everywhere, new locations or branches needed to be added, users accessing the network from their own smart devices, from wherever they are. We see corporate apps, servers, and data in the cloud from minutes ago – alongside older servers from years ago. And we have devices that don't even look like computers are connecting to our networks.

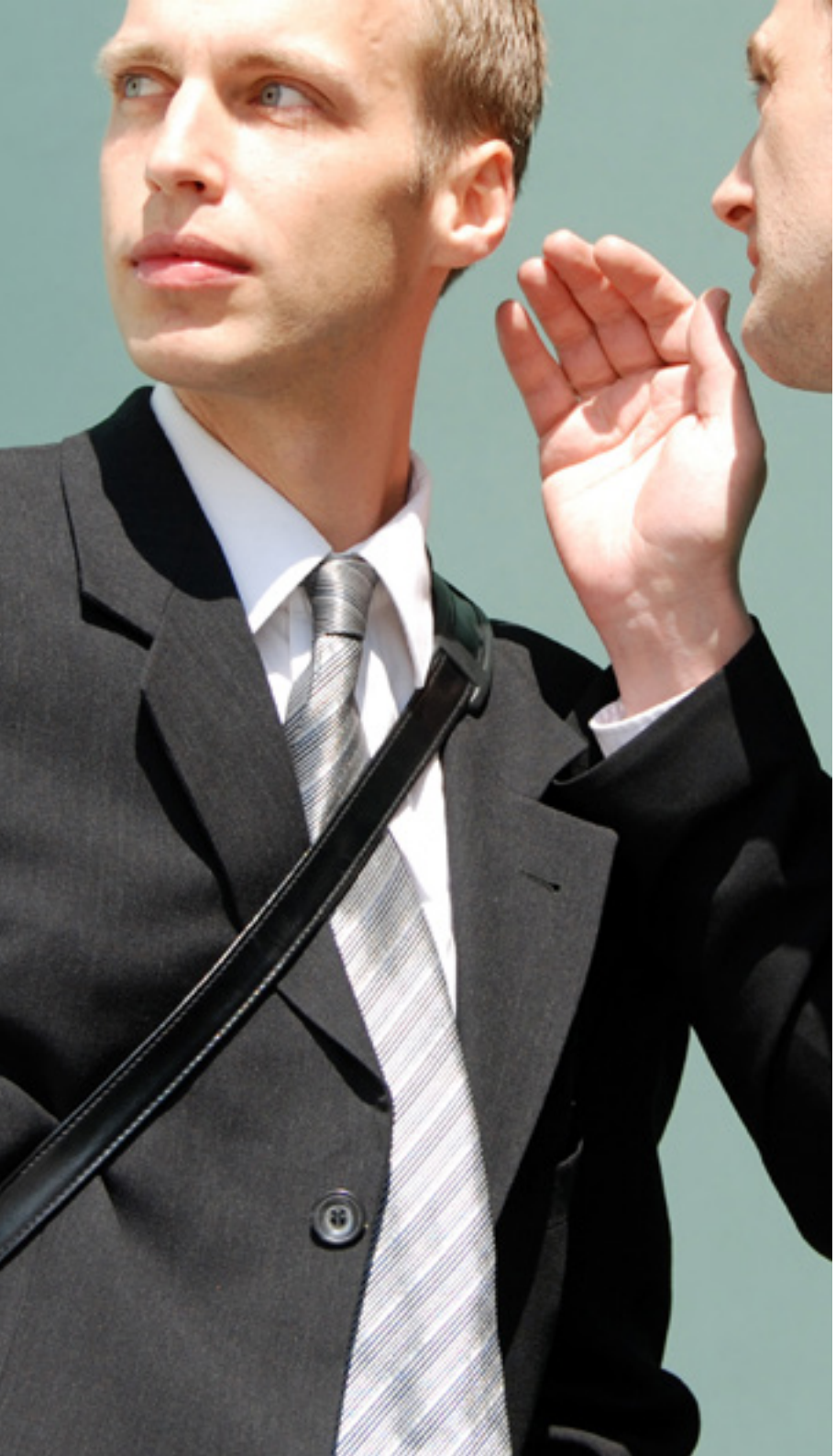
And to thicken the plot, you need to figure out how to get security everywhere to secure this complex infrastructure.

### Sophisticated attackers

Attackers demonstrate a level of sophistication and professionalism that challenges the organization's ability to cope. Motivated by financial gain and sometimes hacktivism, they understand their targets–down to their likes and dislikes and how they conduct business. They exploit any weakness they find ruthlessly. This all means attackers are agile, while companies can't always say the same.

### Unwieldy Security Postures

But our security response to this has us all too often look to a patchwork approach of point products to build a security posture. We see a problem and buy a new security box to address it. This means we end up with unwieldy, ineffective security postures thanks to the dozens of products we patch together that were never designed to work or fit together – just further worsening our Frankenstrucutre problem. This undermines our need to get more effective security.



# Digitization: Opportunity, Challenge or Threat?

The digital economy is fueling new business opportunities through greater speed, efficiency, and agility. To capture opportunities made possible by digitization, businesses of all sizes must also engage in a secure way. To do this, security must be effective and simple, present from the network out to mobile users and endpoints to the cloud.

Speed is also a critical factor in security. For example, the time it takes to detect and respond to a breach, and the ability to act in real-time, is fundamental in a business environment. Security should be a continuous process, always turned on, as opposed to outdated models where scheduled, point-in-time detection prevailed.

Modern networks constantly evolve and spawn new attack vectors including: mobile devices, web-enabled and mobile applications, hypervisors, social media, web browsers, home computers, and even vehicles. Further, mobility and the cloud have created a constantly morphing set of users, locations, applications, access methods, and devices. All of these considerations create greater opportunities for attackers who are becoming increasingly sophisticated and professional in their approach.

## Common security challenges:

- **Too Many Point Solutions:** Some organizations have 40-60 different security solutions that don't interoperate. Investing in an architecture with piece designed to integrate can improve security.

- **Slow Time-to-Detection (TTD):** Industry average rate is 100-200 days to detect a threat that is present. Cisco's advanced security solutions can help reduce average TTD to 13 hours.

Digitization brings many opportunities for businesses and, most importantly, increased efficiencies for the end users. However, companies should not only be aware but committed to addressing the security challenges that arise in this new landscape.

# Securely Enjoy New Business Opportunities

Today's threat landscape is nothing like that of just 10 years ago. Simple attacks that caused containable damage have given way to modern cybercrime operations that are sophisticated and capable of causing major loss and disruption to organizations.

Some of these advanced attacks are very difficult to detect, may remain in networks for long periods of time, and amass network resources to launch attacks elsewhere. In other occasions, such as in ransomware attacks, the breach happens in a much shorter period of time but it can be so devastating that it can bring the affected organization to a complete standstill in operations. Recent ransomware variations managed to encrypt entire systems and data was not returned to the victims even after the ransom was paid.

Vendors encourage security organizations to pile on point solutions to address a plethora of needs. Typically, this complex patchwork of products doesn't fit or work together–creating gaps, management headaches and inefficiencies that attackers can exploit. In addition, point solutions may contain features often overlap, meaning companies often pay for redundant, unnecessary security functionality. This all yields severely unwieldy, compromised security postures.

Traditional antivirus and firewall methods that rely exclusively on detection and blocking for protection are no longer adequate. We believe that effective security is achieved through solutions that are simple, open and automated which we'll discuss in a bit.

# Cybersecurity: A Growth Engine for the Digital Economy

Connected world, digital business, IoE – they all disrupt the traditional ways of doing business. When evaluating the implementation of new technologies – whether to pilot a new business model or additional services – organizations need to build security into all business-critical areas from the start. It is important to consider how effectively legacy security solutions will secure these new environments.

Only Cisco has the breadth of technology and talent to build an Integrated Threat Defense that sees a threat once and blocks it everywhere. Supported by this capability, organizations can advance their business more quickly and capture opportunities ahead with the confidence that they are secure.

An Integrated Threat Defense clearly increases effectiveness against advanced attacks. But it also allows security to become an enabler for businesses to take full advantage of opportunities presented by digitization.

# Truly Effective Security is Simple, Open and Automated

Cisco delivers truly effective security with a best of breed portfolio, world-class threat intelligence, leading services organization and architectural approach with products that fit together for more effective and simpler security that yield a force-multiplier of effectiveness.

## Simple

We work to abstract what's complex to make the most effective technologies simple. This doesn't mean we are not also incredibly innovative and technical. It just means our innovation will deliver simpler security experiences to customers – be it simple to deploy, scale or manage.

## Open

Cisco builds products designed to interoperate at every level of the security stack, not only across our portfolio but also with products provided by others. Open offerings set the stage for an ecosystem that integrates to become vastly more powerful as products are used together.

## Automated

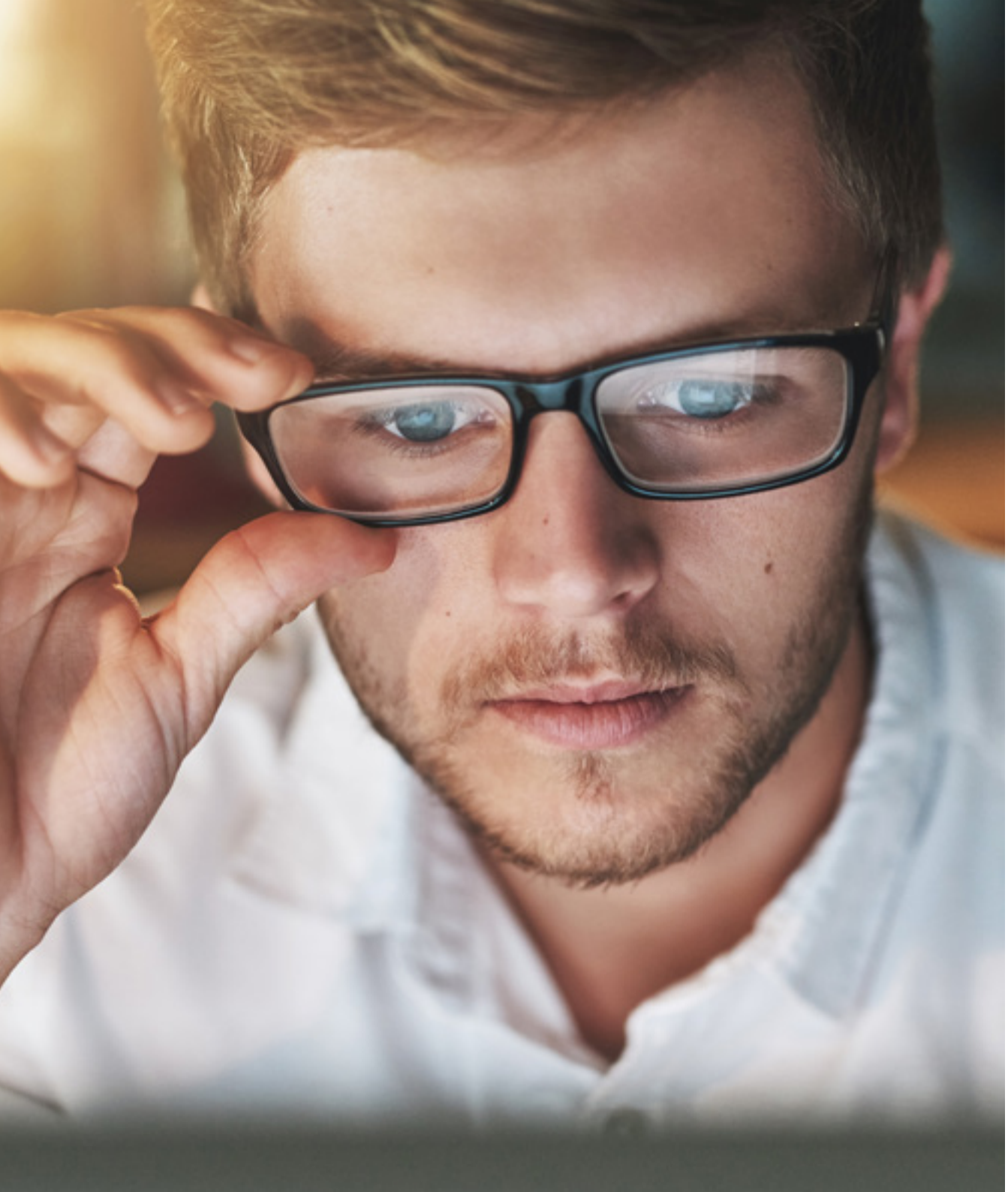
Cisco solutions are automated to yield a force multiplier of effectiveness, removing the burden from teams and empowering organizations with faster time to detect and respond.

# Health Check: Does Your Organization Have Any Security Gaps?

- **Fragmentation:** organizations have an average of 45 different security vendors in their IT environments
- **Slow response:** 60% of breached data is stolen in hours and 75% of attacks take only minutes to begin data exfiltration but take much longer to be detected
- **Slow detection:** 54% of breaches remain undiscovered for months or even years
- **Low Visibility:** 90% of organizations are not fully aware of all their network devices
- **Vulnerable mobile apps:** 92% of top 500 Android apps carry security and/or privacy risks
- **Silos:** 5–10 times more cloud services are being used than known by IT

## Some important questions to ask when going digital:

- Can our security meet the requirements of a digital, connected business?
- Do we know which are our business-critical services and systems and understand the impact a security breach could have on them?
- Can we respond fast enough if we get attacked?
- Are we prepared to adapt our security strategy to new business models and attack vectors, as our IT landscape continues to change?
- In an evolving threat landscape, how do we improve our ability to continuously protect against attacks and increasingly sophisticated threats?
- How are we going to reduce complexity and fragmentation of our security solutions?



# Security in the network DNA

## Network as a Sensor and an Enforcer: Grow Your Business Securely

What if you could use your network and all the traffic information you already have to build a stronger security architecture? This is already possible.

For example, the network may be used as a sensor, to enhance threat visibility. In this case, suspicious traffic flows are flagged and analyzed to more accurately identify hostile behavior and potential threats. The network can also be an enforcer, by dynamically reacting to these anomalies. It can help enforce security policies to reduce the overall attack surface, detain malware and quarantine any contaminated devices. Having the network as an enforcer also enables a high level of automation – making it faster to analyze vast amounts of data related to network behavior – to contain threats faster and give insight into threat evolution.

The network itself can help implement advanced threat protection and reduce time-to-detection and time-to-response.

# About Cisco

Cisco is building truly effective security solutions that are simple, open and automated. Drawing on unparalleled network presence as well as the industry's broadest and deepest technology, services and talent, Cisco delivers ultimate visibility and responsiveness to detect more threats and remediate them faster. With Cisco Security, companies are poised to securely take advantage of a new world of digital business opportunities.

Contact your local Cisco Security team for more information.


**Americas Headquarters**
Cisco Systems, Inc.
San Jose, CA

**Asia Pacific Headquarters**
Cisco Systems (USA) Pte. Ltd.
Singapore

**Europe Headquarters**
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices



Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)