Five Network Security Challenges That Have IT Banging Their Head Against A Wall

How Complexity and the Explosion of Devices Make It Difficult to Secure the Network

We live in "interesting" times—an age of explosive growth when it comes to the numbers and types of devices that reside on enterprise networks. Managed devices with security agents on board, such as conventional PCs, laptops and corporate-owned smartphones, are becoming an ever-decreasing slice of the pie as Internet of Things (IoT) and operational technology (OT) devices join networks by the millions or billions every year.

Add to that all kinds of endpoint applications, operating systems and virtual instances that must be continuously monitored to make sure they don't go rogue. What's more, all this activity is happening on greatly expanded, tremendously complex extended networks. **To say that IT security professionals have "challenging" careers is a gross understatement.**

But all is not gloom and doom. What follows are five key challenges that can be effectively met by acquiring one overarching capability: continuous device visibility.

Challenge 1 Devices are diversifying as their numbers explode

Gartner estimates that 20.4 billion IoT devices will be in use worldwide by 2020.[2] Gartner also forecasts that by 2020 more than 25 percent of identified attacks in enterprises will involve the IoT.[3]

These predictions are scary all by themselves, but consider this statistic derived from a recent ZK Research IT Priorities survey: IoT devices are deployed by OT teams in 60% of cases, which means that IT teams are likely to be unaware of their existence. The author of the ZK Research study concludes that a lack of visibility into these devices combined with the inability to detect the type of device being used creates enormous challenges for IT and security teams—the people who are accountable for monitoring and segmenting these devices.[4]

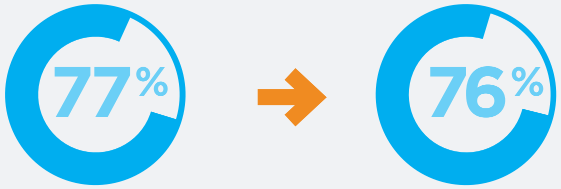
60%

OT Deployed | **IT Unaware**

IoT devices are deployed by OT teams in 60% of cases / IT teams are likely to be unaware they exist.

ZK Research study

IoT is Forcing IT to Rethink Network Security



say increased IoT device usage creates security challenges.

reassessing how they secure their networks.

Forrester Research

It's no wonder that, according to Forrester Research, 77% of companies admit that increased usage of IoT devices creates significant security challenges, and that 76% of those companies are reassessing how they secure their networks.[5]

[1] Endpoint Protection and Response: A SANS Survey, https://www.carbonblack.com/wp-content/uploads/2018/06/20180605_Survey_Endpoint-2018_Final.pdf
[2] Gartner press release, https://www.gartner.com/newsroom/id/3598917
[3] Gartner press release, https://www.gartner.com/newsroom/id/3291817
[4,7,8] ZK Research, Dynamic Network Segmentation Is a Must-Have for Digital Businesses [link?]
[5] Forrester Research, Fail to Plan, Plan to Fail, https://www.Forescout.com/wp-content/uploads/2017/11/Forrester-Survey-Fail-To-Plan.pdf

If Gartner is right that 25% of identified attacks will involve the IoT by 2020. What about the other 75%? You can bet that a large percentage will be attacks related to endpoints that, like IoT devices, aren't covered by traditional security practices and can't be seen by conventional security tools: virtual machines, for example.

They rarely have intrusion prevention or other security in place at the instance level. Industrial control systems and other OT systems are also in this vulnerable category. They used to be "air-gapped" when they ran independent of and parallel to IP networks. But now that nearly everything is connected to the Internet, these endpoints are vulnerable to attack like everything else.

Like most IoT devices, OT systems and VMs are joining extended networks in huge numbers and rarely have security agents on board. Even managed PCs and smartphones that do have agents installed are at risk if those agents aren't running properly, if patching isn't up to date, or if unauthorized applications are operating undetected.

What's needed is the ability to see and continuously monitor devices of all kinds, with an assist from infrastructure. Ideally, even without agents, you should be able to see into devices by collecting information from switches, wireless controllers, virtualization infrastructure, cloud providers and third-party tools on your network. It's the only way to make devices and network components comply with your organization's security policies.

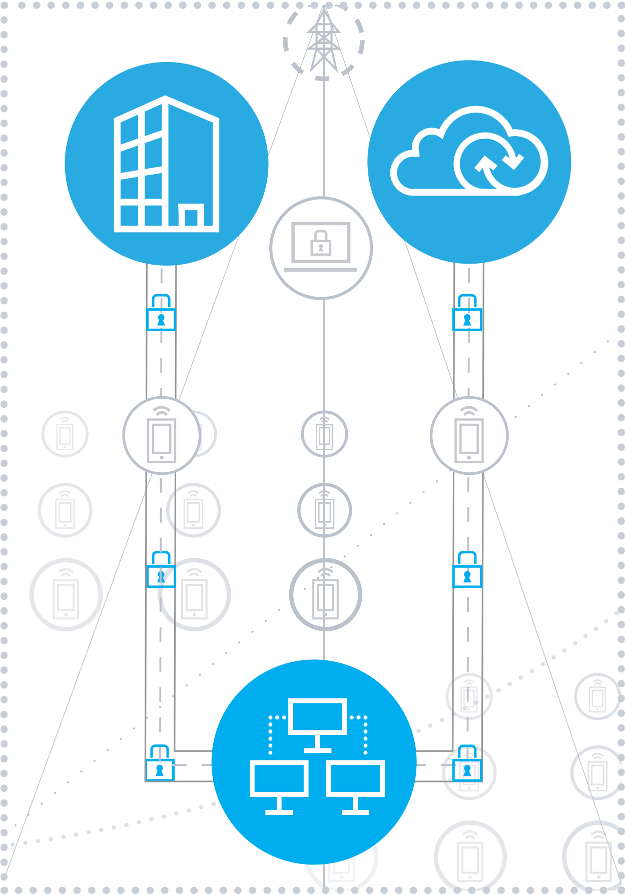
Keep in mind that these are only the user endpoints that companies are aware of. There are probably many, many more.

Challenge 2 Network perimeters are vaporizing (and so is control).

The Internet punched traditional perimeter-based corporate networks full of holes, and now cloud computing is dissolving what remains. Today's enterprise networks are distributed far and wide, and organizations everywhere are signing up to take advantage of self-service, on-demand SaaS, PaaS and IaaS cloud computing services. Some are even circumventing conventional IT services altogether.

With corporate compute assets becoming widely dispersed and less likely to be on premises or tightly managed as in pre-cloud days, IT professionals' security and overall management responsibilities are greater than ever.

Since old-style network boundaries are going away, perimeters now must be thought of in terms of the connected devices, applications and corporate data themselves—each asset must be secured within its own perimeter, wherever in the extended network environment they may be. IT pros need to have knowledge and leverage when it comes to securing what belongs to the organization—even if it's virtualized and residing on someone else's platform. Regulations still need to be complied with, and policies have to be upheld.



What's required is an integrated security strategy based on tools that can readily traverse the various realms of today's distributed IT environment.

So, how do you scale security policy across the campus, data center and cloud? According to the Enterprise Strategy Group (ESG), a good starting point is to gain the same type of detailed visibility of virtual instances that's required of physical devices. This means being able to discover, classify and assess virtual endpoints within private clouds and software-defined data centers (SDDC).

The challenge is similar to that of discovering agentless IoT and OT devices. Agentless methods are now available that can provide granular details of virtual assets. ESG also recommends segmenting these workloads to securely control them. We'll cover the segmentation challenge a little later.

A full 79% of security professionals told ESG that network security is more difficult today than it was two years ago.*

ESG, https://Forescout-wpengine.netdna-ssl.com/wp-content/uploads/2017/08/ESG-Forescout-and-the-Software-defined-Perimeter-White-Paper.pdf

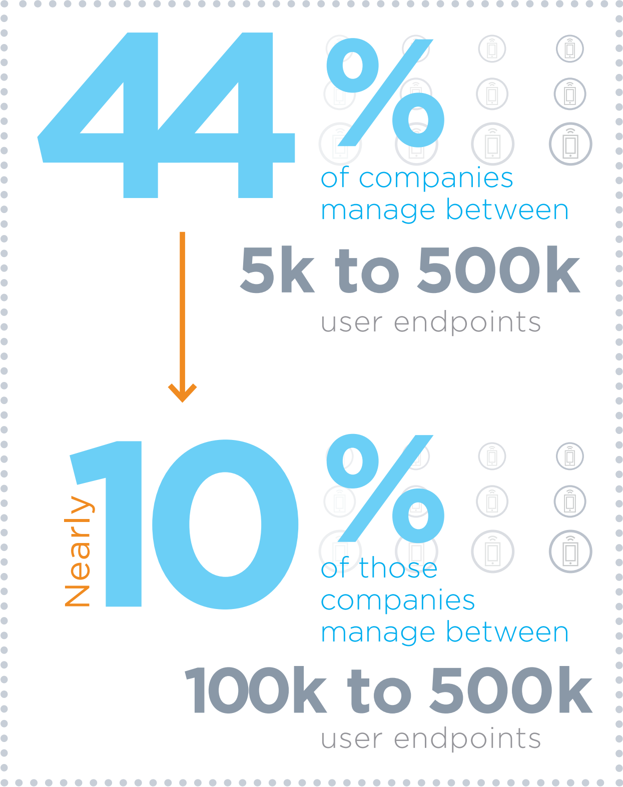
Challenge 3

Inventories are becoming increasingly inaccurate

According to a recent study by the SANS Institute, 44% of companies manage between 5,000 and 500,000 user endpoints. Nearly 10% of those are managing networks of 100,000–500,000 user endpoints.[5]

Those endpoints are likely to include IoT devices with default passwords straight out of the factory; industrial control systems that can be hacked and potentially put entire supply chains out of commission; HVAC systems that can be manipulated; and PCs with old, unsupported OSes that can be easily commandeered. They're all out there, and they all pose serious risks—unless you have access to up-to-date, real-time information about your organization's compute assets.

And that's where an accurate IT asset management solution (ITAM) that features a configuration management database (CMDB) can prove to be extremely valuable. However, "accurate" is often a relative term.



44% of companies manage between 5k to 500k user endpoints

Nearly 10% of those companies manage between 100k to 500k user endpoints

SANS Institute

ITAM and CMDB solutions share a fundamental need for asset discovery and situational awareness, yet these solutions are often plagued by the inability to see network-connected devices in real time due to legacy discovery methods that can't detect IP-addressed endpoints, and which produce gaps in asset visibility. **In fact, most ITAM and CMDB solutions are ineffective at automated asset discovery, which necessitates costly (and often inaccurate) manual true-up detection efforts to close discovery gaps and maintain a trusted baseline of assets.**

[5] Forrester Research, Fail to Plan, Plan to Fail, https://www.Forescout.com/wp-content/uploads/2017/11/Forrester-Survey-Fail-To-Plan.pdf

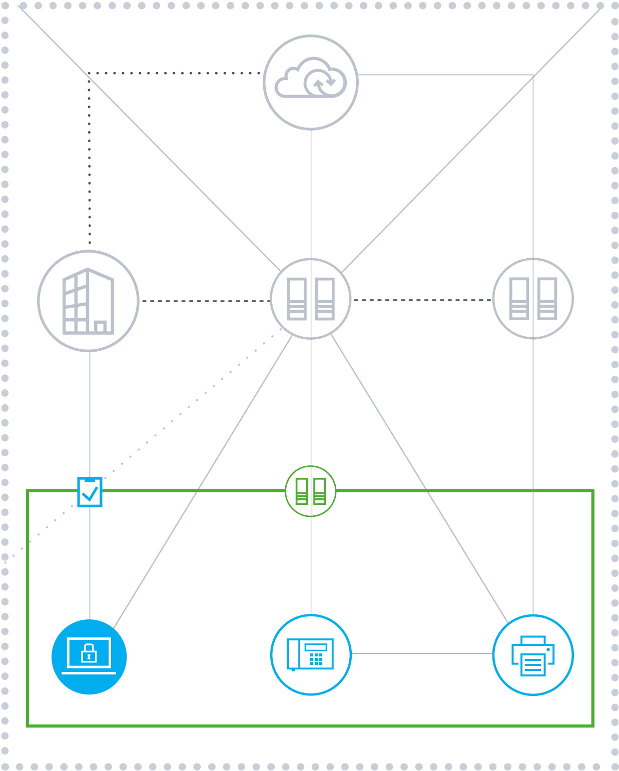
To establish a trusted data set, organizations need an automated way to incorporate current data into ITAM and CMDB solutions. That requires a solution that provides visibility of IP-addressable assets on the network in real time, monitors IT asset and configuration item (CI) attributes consistently, and feeds accurate asset information to a multitude of dependent services and solutions. Otherwise, it's a matter of garbage in, garbage out, not to mention decreased efficiency and increased risk when it comes to responding to threats.

Challenge 4

Network Segmentation is a must, but how do you do it right?

Until recently, network segmentation had a bad rap. It was unpopular largely due to complexity of design and installation as well as concerns that segmentation could lead to slowdowns or glitches in business-critical services. Besides, IT personnel and IT systems couldn’t see such a large percentage of connected devices that the point of deploying segmentation technology wasn’t crystal clear. And segmentation used to require IT staff to manually update network access rules as new devices connected to the network. It was, in a word, painful.

In the rare event that malware infiltrates the network through a compromised device, network segmentation can minimize the damage by limiting the user’s (or device’s) lateral movement. Access is granted only to those corporate assets that a users’ profiles entitle them to, and if a user/device doesn’t comply with your security standards, he/she/it doesn’t gain access. Also, regarding especially vulnerable systems such as agentless IoT and OT endpoints or point-of-sale (POS) systems, segmentation lets you confine and continuously monitor them on their own network segments.



Today there are tools available that can automate security segment assignment based on deep endpoint inspection without agents, and can maintain access enforcement using continuous monitoring and policy-based assignment of ACLs and VLANs. In fact, network segmentation technologies are also available today that provide real-time user and device context to next-generation firewalls. This enables IT organizations to implement dynamic network segmentation and create context-aware security policies within their next-generation firewalls based on endpoint context. Implementing dynamic network segmentation will not only improve your security posture it can save IT time and money. In 2016, an IDC study on network segmentation found that the value of higher productivity created by network segmentation was $1,094 per device per year over a five-year period.[7] That same study calculated that businesses will save an average of $2,058 per IoT device per year using segmentation.[8]

[7,8] ZK Research, Dynamic Network Segmentation Is a Must-Have for Digital Businesses [link?]

Challenge 5

Getting executive buy-in and budget

Speaking of challenges, perhaps the biggest is convincing management that you are going to need $$$$$ for yet another network security tool. That's not an easy sale anymore, if it ever was. **On average, network security teams manage up to 15 tools,[9] meaning companies are spending a lot of money—and a lot of time—buying, deploying and learning about those tools. And many are isolated, single-purpose solutions.**

Of course the problem is, one more tool could be the tool—the one that, by providing device visibility and real-time continuous monitoring capabilities across heterogeneous environments, can prove to be the ultimate platform for securing the network. Hypothetically speaking, this security tool would have a good chance of convincing management to part with cash because it can check all of the following boxes.

All of this is a lot to ask, but it can be done. Cybersecurity solutions have matured tremendously in recent years. The technology you're looking for exists.

Your Next Security Tool Should Check All the Boxes

- ✓ Reduce the size of your attack surface
- ✓ Decrease incidents of network-related security breaches
- ✓ Detect and identify significantly more devices on the network than previously known
- ✓ Integrate with existing security solutions, sharing intelligence and automating and accelerating threat response
- ✓ Enhance the value of the security tools you already have in place
- ✓ Integrate with systems you expect your organization to acquire
- ✓ Boost employee productivity
- ✓ Improve overall IT efficiency
- ✓ Prove its value in days or weeks rather than months or years

[9] https://www.riverbed.com/document/fpo/Riverbed-EMA-NetworkMgmtMegatrends-2016-RR-SUMMARY_CS1.pdf

The bigger challenge behind these 5 challenges

The five challenges listed above are all pretty daunting. But each one, if unresolved, can lead to the ultimate challenge: a cyberattack that results in operational problems, stolen data, brand reputation damage, massive fines, public safety issues—the list goes on.

Prevention is the key and, first and foremost, it requires device visibility and real-time continuous monitoring.

To Learn More

<) FORESCOUT

Device Visibility: The Key to Reducing Risk and Improving Your Security Posture

Six Ways to Enhance Security with 100 Percent Device Visibility

Securing network infrastructure continues to grow more complex by the day. This complexity is driven by the phenomenal growth of IoT devices, platform diversity, cloud adoption and IT and OT convergence. The vast majority of new devices joining your networks aren't designed to support management agents—creating a serious visibility and risk gap. And this gap further widens as cloud computing extends to the furthest corners of the distributed network.

Of course, what you can't see can kill you. You need a way to discover devices whether they have agents on board or not, whether they're physical or virtual—regardless of where they're located. You also need continuous, real-time monitoring and the ability to profile and classify devices the second they attach to your network.

Closing this visibility gap is the most effective way to achieve a positive impact on your network security and risk mitigation efforts. Here are six opportunities to do just that using absolute visibility:

<) FORESCOUT | Device Visibility: The Key to Reducing Risk and Improving Your Security Posture | 1

Six Ways to Improve Your Security Posture

Learn how device visibility enables you to drastically reduce risk and improve your security posture.

[Device Visibility: The Key to Reducing Risk and Improving Your Security Posture]

<) FORESCOUT

EXPERIENCE THE DIFFERENCE

of The Forescout Visibility Platform

Your guide to achieving real-time visibility and network security for all your devices everywhere.

Ready to Solve Your Toughest Security Challenges?

Download the interactive Forescout Solutions Guide to learn how to solve your network security challenges.

[Forescout Solutions Guide]

Forescout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591