SECURITY+

Featured Articles

4 The Paradox of Cyberthreats

8 The User: Always Your Weakest Link

11 Rethinking Data Security with a Risk-Adaptive Approach

Inside this edition

3 — **The Ultimate Guide to Security Awareness Training**

Learn how to protect your organisation from the techniques hackers use to gain entry to your systems.

4 — **The Paradox of Cyberthreats**

We look into the past year of ransomware outbreaks.

6 — **Debunking The Myths Around SD-WAN**

The top 5 myths around SD-WAN and key insights you need to know.

8 — **The User: Always Your Weakest Link**

Charting the rise of phishing attacks, and the role of the user.

9 — **Delving into the World of Business Email Compromise (BEC)**

An analysis of the trends in BEC and what to look out for.

10 — **Teaching the Big Boys to Share Big Data**

Big Data and Big Data Analytics (BDA) are no longer the preserve of the enterprise - everyone can benefit from essential insights into their data.

11 — **Rethinking Data Security with a Risk-Adaptive Approach**

Megatrends of Cloud Based Applications and mobile devices which have seen a benefit for companies with improved agility and innovation.

12 — **Securing the Cloud: The Future of Authentication**

Read our survey to find out what lies in the future of multi-factor authentication.

14 — **Securing the Whenever, Wherever Workforce**

Securing SD-WAN to protect your workforce in the BYOD era.

16 — **How to Build a Security-Centric Culture in Your Company**

Keeping security posture at the core of each business unit.

18 — **5 Tips to Avoid Public Wi-Fi Security Dangers**

Advise on overcoming public Wi-Fi fears.

19 — **Safeguarding – Your moral duty of care?**

Approaching GDPR and data security with morality over obligation.

20 — **Connecting the Internet of Things**

Best practices to prepare for and manage an IoT deployment at a fundamental level.

22 — **The Forgotten Hero – Patching**

Why patching is the superpower your organisation needs.

Cyber Risk Aware
Creating your human firewall!

The Ultimate Guide to Security Awareness Training

Research released by the Global Cyber Security Capacity Centre affirms the indisputable importance of staff training in mitigating security risk. We've worked with clients across the globe in building security-training programs that safeguard their systems and support their teams. In our guide, learn about the following:

- The techniques hackers use to gain entry to your systems
- The threats facing your company and its customers
- The value of a security awareness training program
- The key elements of a robust security awareness training program
- A best practices checklist for commencing and sustaining security awareness training

Constant training is needed to meet an evolving threat: The number and sophistication of attacks is increasing quickly. Companies have to be engaged and pro-active in order to stay ahead.

Prevention is always better than looking for a cure: Most successful attacks are facilitated unwittingly by untrained staff members. The key to ensuring that your technical defences work is to have employees that can detect suspicious behaviour and react in the right way.

Engage your staff proactively in protecting your enterprise: Boring tick-in-the-box training is not going to get the job done. You have to deploy a variety of content, simulations, reminders and assessments to keep your team engaged and committed to protecting the enterprise.

What makes for a successful security awareness training programme? Communications, and getting all departments working together is a key start. Conduct random simulations; if you don't test, you won't know until it's too late. Commit to measurement and always use relevant and current data.

To download the full Ultimate Guide to Security Awareness Training, visit www.securityplusonline.co.uk

The Paradox of Cyberthreats

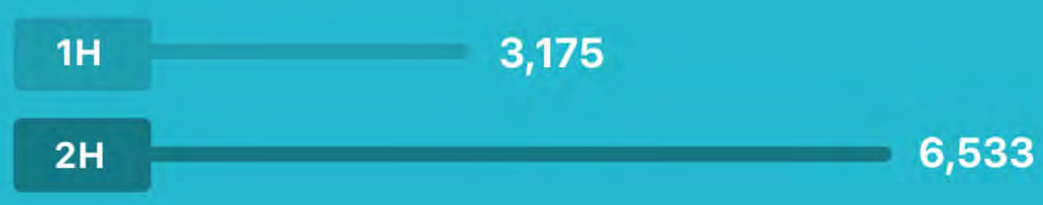
The past year saw massive ransomware outbreaks turn into global events that reportedly cost enterprises billions of dollars. We also saw familiar threats like business email compromise (BEC) continue to be a consistent danger for enterprises. Meanwhile, volatile cryptocurrencies disrupted the threat landscape as their value steeply and quickly rose. To function in this environment, cybercriminals reworked old techniques to take advantage of the crypto-trends and also tried to exploit known vulnerabilities in new ways.

Amid growing awareness of the threat, **BEC scams** are still on the rise

Past cases have emphasized the risk BEC scams pose to all types of enterprises, from large multinationals to small businesses. But despite the increasing awareness, BEC scams still prevailed and grew in 2017. One incident, which cost a Japanese transportation company a reported $3.4 million, happened just in December. This particular scam centred on a popular technique called the supplier swindle: impersonating a third-party supplier and manipulating the company into transferring funds. In another incident reported in July, a number of organisations in Germany received fake memos from "executives" that asked accounting personnel to send funds to fraudulent accounts.

Our data shows a steep rise of about 106 percent in attempts from the first half of 2017 to the second half. Consistent with previous years, the most targeted positions were finance-related: chief financial officer (CFO), finance controller, finance manager and finance director. The most spoofed were high-level executives: chief executive officer (CEO), managing director and president.

Recorded BEC Attempts in 2017



BEC attempts more than doubled in the second half of the year over the first half: comparison of BEC attempts between 1h and 2h of 2017

Adaptable threats exploit known **vulnerabilities** in new ways

Several critical and controversial vulnerabilities were exploited by cybercriminals and used for major ransomware campaigns. Most notably, these included the known ones that were taken advantage of by the EternalBlue and EternalRomance exploits. The former was used in the WannaCry and Petya outbreaks, and the latter was also used in the Petya attacks, and later in the Bad Rabbit incident.

Known vulnerabilities were exploited, as well for purposes other than spreading ransomware. EternalBlue was also used by a cryptominer malware to spread filelessly, and the Linux vulnerability Dirty COW was used by ZNIU to compromise specific Android devices.

A MARKED INCREASE IN ZERO-DAY VULNERABILITIES: COMPARISON OF NUMBER OF ZERO-DAY VULNERABILITIES AND SCADA-RELATED ZERO-DAY VULNERABILITIES BETWEEN 2016 AND 2017

2017 also saw a substantial 98% increase in discovered zero-day vulnerabilities. Moreover, of the 119 zero-day vulnerabilities, all but six were related to supervisory control and data acquisition (SCADA). This increased focus on SCADA is particularly significant since major industrial complexes and critical infrastructures rely on this control system architecture to function. If exploited, zero-day vulnerabilities could result in huge losses and damage.

Ransomware brings about bigger global outbreaks despite fewer major players

The number of new ransomware families rose 32% from 2016 to 327, showing that there were still active ransomware developers trying to take advantage of a plateauing trend. However, the ransomware-related threats detected by the Trend Micro™ Smart Protection Network™ security infrastructure went in the opposite direction and dipped 41%. Apparently, only a select few of these new families actually made an impact in 2017.

The ransomware events that did affect users were significantly larger. These widespread attacks struck multiple countries, and reportedly resulted in billions of U.S. dollars in damage. In addition to WannaCry and Petya - the two most notorious - there was the more recent case of Bad Rabbit; in October, the ransomware hit a number of enterprises across Russia, Eastern Europe and the U.S.

This was a marked difference from 2016, in which more ransomware incidents were reported, but the scale of the damage was typically contained to local offices, and the ransom demanded was just in the tens of thousands of dollars.

PREVAILING RANSOMWARE FAMILIES: TOP RANSOMWARE FAMILIES IN 2017 REMAINING FROM 2016

Ransomware remains a clear and steady threat as many old families still affect users worldwide. Meanwhile, the more recent virulent outbreaks show that the new families are growing more sophisticated and hitting larger targets. Developers are constantly experimenting, trying to find profitable strategies. In 2017, they used diverse new methods; for example, more had been using fileless infection and pre-execution machine-learning evasion techniques in addition to taking advantage of old vulnerabilities.

More ransomware families emerged in 2017: Comparison of total number of new ransomware families seen.

247
2016 NEW FAMILIES

327
2017 NEW FAMILIES

Fewer major players despite increase in new ransomware families: Comparison of total number of detected ransomware-related threats

1,078,091,703 2016 RANSOMWARE-RELATED THREATS

631,128,278 2017 RANSOMWARE-RELATED THREATS

Cryptocurrency's meteoric ascent inspires new mining malware and other threats

The value of cryptocurrency, particularly bitcoin, skyrocketed in the latter half of 2017. In the beginning of July, 1 bitcoin was valued at around $2,500, and by Dec. 31, it was valued at over $13,800. That steep and quick increase apparently prompted cybercriminals to target cryptocurrency through different methods. Some used social engineering attacks to directly target cryptocurrency wallets, while others evolved old ransomware threats to do the same. There were even attempts to mine cryptocurrency through mobile malware, despite the improbability of gaining any substantial amount by that means.

- **Apps with mining malware**
- **Mining bots spreading through social media**
- **Cryptocurrency wallet hacking**
- **Compromised "tech support" websites**
- **Websites using mining scripts**
- **Exploit kits dropping mining malware**
- **Ad networks delivering miners**

Some businesses had tried to capitalize on cryptocurrency by using mining software as alternatives to web advertising, but cybercriminals were also quick to take advantage. In mid-2017, cybercriminals started abusing the most popular of the open-source mining tools, Coinhive. By November, an abused variant of the Coinhive miner ranked as the sixth most common malware in the world, even though it was intended to be a legitimate alternative method of making money for websites.

These are particularly relevant threats since businesses are starting to use cryptocurrency and even launch their own; governments, including those of Venezuela and Dubai, United Arab Emirates, are also establishing their own cryptocurrencies. Security solutions with high-fidelity machine learning, web reputation services, behaviour monitoring and application control could help minimise the impact of these threats.

Debunking The Myths Around SD-WAN

Regardless of industry, today's enterprises constantly strive to improve productivity and reduce costs. Software and commodity internet connections now play a key part in achieving both: SD-WAN (short for software-defined wide area networking) represents a revolutionary way of thinking about how to connect locations.

As with many technologies, what started off as hype for the bleeding-edge is maturing into real solutions that can make an impactful difference, even for large, distributed organizations. With every new way of thinking comes misconceptions or "myths" that spread like wildfire before they are properly vetted.

It's time to debunk these SD-WAN myths. A Secure Enterprise SD-WAN approach is here, with SD-WAN connectivity and NGFW security managed together at scale to connect and protect your organisation like never before.

FORCEPOINT

Myth #1 - SD-WAN is just about replacing MPLS to save money

MPLS services are expensive. They can even be difficult to get rid of, since they are typically bought as part of a long-term contract. But beyond putting a cap on spending, there is a better reason to implement SD-WAN: it's far more versatile than MPLS.

Using fast, commodity broadband instead of slower, expensive MPLS not only can save money, it can provide a "10x" increase in capacity. It provides resilience for business continuity, protecting sites from the legendary enemy of buried cabling—the backhoe. SD-WAN gives your expanding organisation options for how to connect new locations where adding MPLS capacity is costprohibitive, slow to provision or may not even be available.

**SD-WAN does more than save you money.
It provides agility and options, boosts capacity,
improves resiliency and accelerates new locations.**

Myth #2 - SD-WAN takes the place of the internet

Some SD-WAN vendors try to sell their customers proprietary network connections and provide a front-end private network for getting to the internet. Such link-specific solutions are often only available in limited geographies and can be very slow to provision. SD-WAN is about choices, enabling you to mix and match whichever links are most appropriate for each location (e.g., cable, DSL, fiber, 4G/LTE). It provides a way to facilitate and manage connectivity, but should never attempt to limit or take the place of any websites or internet applications.

**SD-WAN doesn't replace the internet, but
does facilitate connectivity**

Myth #3 - SD-WAN eliminates the need for on-premises hardware

SD-WAN is frequently used to direct traffic for particular applications across specific links. This is especially important for reducing the latency needed to connect to highly interactive cloud apps like Office 365 while increasing the available bandwidth. It can be used to enforce techniques like encryption, which provides privacy for accessing cloud apps that aren't already relying on SSL/TLS and keeps data safe in transit.

But even with SD-WAN, you still need on-premises equipment to plug into your various network links. Strong security is an absolute must no matter where you're attached to the internet, and a firewall with built-in intrusion prevention and cloud security technologies

SD-WAN has some equipment at each location to plug into your ISP links and potentially provide necessary security.

Myth #4 - SD-WAN solutions all come with high availability, easy manageability and excellent security

SD-WAN has exploded in popularity, but that doesn't mean that all SD-WAN vendors do the same thing. Some only connect organisations or can only handle a few locations, and therefore have management systems geared towards a relatively small number of sites. These vendors may wrongly assume that all sites use the same types of connections.

A new generation of enterprise-grade SD-WAN solutions is emerging that:

- Connects thousands of locations over whatever type of network links are available and appropriate for each site
- Provides always-on resilience for around-the-clock productivity
- Tightly integrates security with connectivity to prevent gaps
- Offers 360° visibility into user behaviors and the flow of data everywhere, from branches to main offices, data centers to the cloud
- Enables common policies to be expressed once and reused automatically wherever needed
- Expresses special requirements for particular locations efficiently without disrupting normal operations
- Automates connectivity tasks like setting up VPNs among sites so that new sites can be added quickly and reliably
- Pushes policies to modify how sites are connected or secured
- Updates networking and security infrastructure without taking sites offline

Look for secure enterprise SD-WAN solutions for efficiency at scale.

Myth #5 - SD-WAN already has security built into it

According to Gartner, branches need the same level of enterprise-grade security that is employed at headquarters for primary internet gateways. Many first-generation SD-WAN solutions enforce encryption of traffic over commodity broadband links using Virtual Private Network (VPN) technologies. This keeps data and communications between different sites private, but doesn't make the sites more secure.

The new generation of enterprise-grade SD-WAN solutions has security that is fully distributed, instead of centralized like that of hub-and-spoke network topologies. This keeps attackers from sneaking into your stores, branches or remote offices and protects the use of SaaS applications. Advanced Secure Enterprise SD-WAN uses techniques such as "service chaining" to apply security capabilities like web traffic protection and CASB to automatically secure data transmitted to cloud-based apps.

The User: Always Your Weakest Link

The Verizon Data Breach Investigations Report (DBIR) is one of the most respected annual reports in the security industry.

Every year, the Verizon Research, Investigations, Solutions and Knowledge (RISK) team, one of the largest IT investigative entities in the world, shares deep insights into the state of cybersecurity for the year, including the largest trends.

In 2017, the team found that phishing is used in more than 90% of security incidents and breaches.

And at equally alarming rates, users with their many devices are falling victim to ransomware and other malware via these user-targeted attacks. According to Verizon, 30% of phishing messages were opened in 2016 - up from 23% the year before - and in 12% of those events, users clicked to open the malicious attachment or link.

The Verizon RISK team highlights the rise of a three-pronged phishing attack:

> The user receives a phishing email with a malicious attachment or a link pointing to a malicious website.

> The user downloads malware, which attackers can use to look for secrets and internal information, steal credentials to multiple applications through key logging, or encrypt files for ransom.

> Attackers can also use stolen credentials for further attacks: for example, to log into third-party websites like banking or retail sites.

Which of the following was targeted as part of this external attack?

Forrester's Global Business Technographics Security Survey. 2016

So, how is it that even the biggest corporations out there, with, what one can only imagine, are high-powered security tools in their arsenal, still fall victim to these attacks?

For one thing, many of the tools in place aren't protecting the most vulnerable assets.

For its 2016 Global Business Technographics® Security Survey, Forrester surveyed 192 network security decisionmakers whose firms had an external security breach in the past 12 months (1,000+ employees). As part of that survey, they asked respondents which aspects of their infrastructure were targeted in the external attack. The results showed definitively that it's the clients and servers in your network that need to be your primary focus - not the perimeter of your IT environment.

Unfocused Security Strategies? They Lead Only to Expense in Depth

Unfortunately, even if you have the tools in place to protect against these threats, they remain just a few of the many you're configuring and managing daily. Network firewalls, web application firewalls, intrusion prevention systems, vulnerability scanners... oh my! Device sprawl is costly, and IT teams spend too much time managing these devices - time taken away from working with Security to protect against and respond to real threats to the environment.

Where Do We Go From Here?

From an IT security prospective, we may think that by blocking access to particular material online it's enough. In reality, if someone really wants to access the information they will typically find a way. However, if that's not through the organisational network or through supplied devices then it's not your concern – right?

It could be argued you have taken all the steps you could to stop access to that information. Therefore if something happens outside of your organisation relating to that individual successfully accessing, and then acting upon, the information you may well be right in thinking you did all you could....

Morally, is this where we as IT professionals, teachers, governors should draw the line and say we did enough? When we consider where that line is, what is driving that decision? Is it purely philanthropic?

With the right tools in place, and a clear understanding of the safeguarding aims, we can do a little more than just the bare minimum. Monitoring of individuals online data is always undertaken with trepidation, but is it the monitoring of that individual's activity and balancing that with their right to privacy that should concern us, or the ways this could potentially restrict academic endeavour, discussion and debate of controversial topics.

Delving into the World of Business Email Compromise (BEC)

Business Email Compromise (BEC) attacks have expanded tremendously over the past few years, with a projected growth of over $9 billion in 2018. The combination of simplicity and effectiveness have ensured that BEC will continue to be one of the most popular attacks, especially for those who lack special tools and knowledge to pull off more complicated schemes.

We looked at BEC-related incidents over a period of nine months (from January to September 2017) to see emerging and present trends from BEC incidents. We examined the tools and techniques cybercriminals use, and analyzed the data to give us an overall picture of what BEC looks like today.

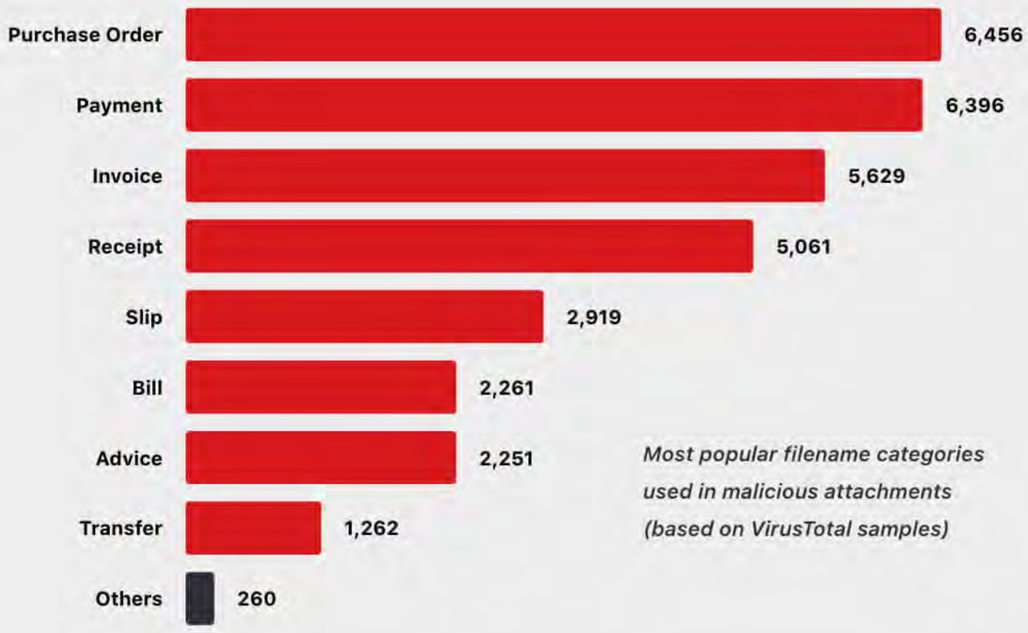
The Internet Crime Complaint Center (IC3) separates BEC attacks into five main categories, but during our tracking efforts, we managed to narrow these even further to two main techniques:

> **Credential-grabbing** - Involves the use of keyloggers and phishing kits to steal credentials and access the webmail of target organisations.

> **Email-only** – Involves an email sent to someone in the finance department (usually the CFO) of the target company. The attackers design the email to make it look as if a company executive sent it, typically instructing the target to transfer money. The transfer request is usually for payment to a supplier or contractor, or as a personal favor.

Credential grabbing-techniques can further be categorised into those that use malware and those that use phishing.

By examining malicious attachment samples that had filenames that could be clearly categorised, we were able to determine the most prominent ones:



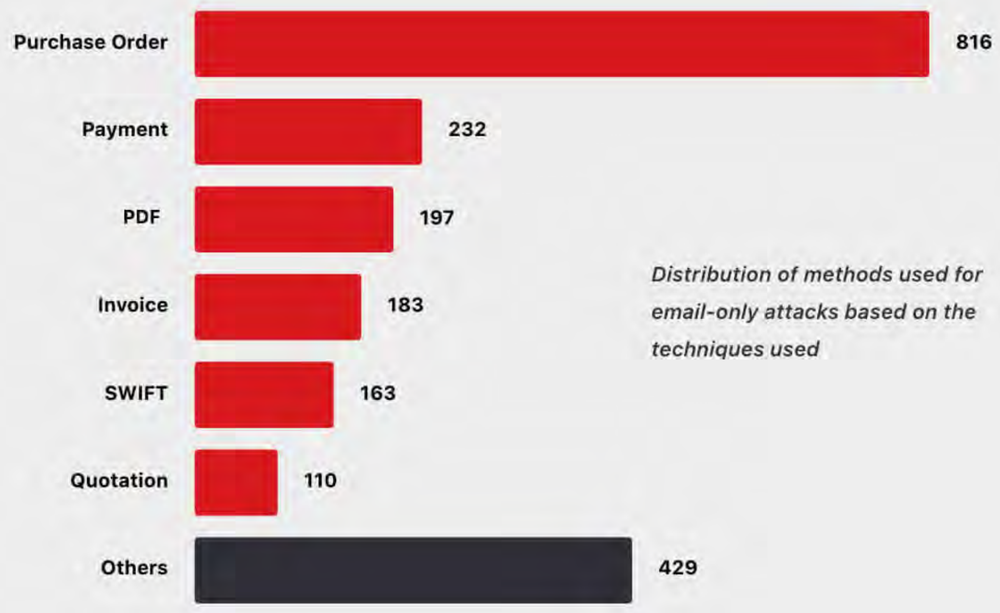
Most popular filename categories used in malicious attachments (based on VirusTotal samples)

Our research into malware-related BEC attacks also revealed two key players that emerged on the scene: Ardamax, which is $50 software that provides a BEC actor basic features that they would need to operate; and LokiBot, a known malware family that is increasingly being used in BEC attacks.

Email-only BEC attacks, on the other hand, use social engineering techniques. While social engineering is a common aspect of most BEC attacks, an email-only attack uses more sophisticated methods to exploit the human psyche. Simply put, these attacks use email designed to look as believable as possible. These kinds of BEC attacks typically involve the clever use of the Subject field, the "Reply-to" portion of the email, as well as where the email comes from.

BEC actors will also create legitimate-looking email addresses designed to impersonate company executives, either by using dodgy free webmail providers or by registering a copycat domain that resembles or references the target company.

The distribution of email-only BEC attacks according to the techniques used can be seen in the chart below:



Distribution of methods used for email-only attacks based on the techniques used

In addition, we also looked at how BEC actors acquire their tools, particularly the phishing websites they used in their attacks. One of the most common methods used by BEC actors involve the use of phishing kits - scampages - as the main source of attacks. Examining these websites allowed us to identify a BEC actor and learn how this individual sourced and utilized his tools.

We found traces of this individual in multiple phishing sites, providing us with clues on how many BEC actors use multiple sites to perform their attacks. They will also typically interact with and have access to underground markets that can provide them the tools they need to pull off effective BEC attacks. Resources are even available to inexperienced BEC actors, as spamming tutorials exist that can help them start their operation. This means that for BEC actors, tools and techniques are easily accessible without having to jump through hoops. This research effort aims to paint a clearer picture of the emerging trends in BEC, the tools and techniques they use, and how individuals and organisations can protect themselves from these types of attacks.

Teaching the Big Boys to Share Big Data

Big Data and Big Data Analytics (BDA) have been on the tip of everyone's tongue for what seems like forever. Initially something that was a nebulous idea, ring fenced for only the biggest and most forward-thinking companies (I'm looking at you, Tech Giants and Telecoms), last year saw an explosion of articles across the web telling businesses that if they weren't using Big Data, they were being left behind. I should note that none of those articles seemed to point towards exactly what the rest of us mere mortals should be using Big Data for...

To their credit, some of the larger consultancy firms have started providing seminars and/or presentations steering people in the vague direction of just signing away your life to get access; definitive answers come at a price, as we all know. This is probably because, unlike a lot of technology that is nowadays forced down people's throats, there is no easy way to tell people exactly what they should be doing to get benefits from BDA. The benefit becomes crucially clear when considered in the context of the individual business needs and landscape.

For example, in the financial services, BDA is absolutely key to their success, not only from a compliance and regulatory perspective, but also because most of us are now banking online, rather than popping down to our local high street branch. This means that it is essential for the analysis of data to remain competitive. The question is: Is it being deployed correctly?

Below are a few potential applications of BDA. These only provide a source of inspiration, unless your business fits neatly in the same sector/circumstances as those referenced:

> **Credit card company and business intelligence -** Hindsight reporting and trailing indicators can only take a business so far, so this company started looking for indicators that could predict loyalty and developed sophisticated models to analyse historical transactions. Using over 115 variables against the data collected, accurate forecasts potential churn were created. The company believes it can now identify 24% of accounts that will close within the next four months.

> **Fast food and video -** This company points cameras on its drive-through lanes to determine what to display on its digital menu board. When the lines are longer, the menu features products that can be served up quickly. When the lines are shorter, the menu features higher-margin items.

> **Supermarket and performance efficiency -** This supermarket chain collected refrigerator-related data points coming off its units and fed them into a dedicated data warehouse. Those data points were analyzed to keep better tabs on performance, gauge when the machines might need to be serviced, and do more proactive maintenance to cut down on energy costs.

What are the options?

Let's start with a big claim. The current issue with utilising BDA in the mid-market is the fact that the two realistic options provide unique challenges that are only solvable at large enterprise.

The first potential option is to invest in the development of a bespoke architecture based on the Hadoop open-source platform. This promises limitless flexibility and the ability to deliver the exact needs, nothing more and nothing less. This sounds amazing in theory, however, as everybody knows, too much of a good thing can be bad.

By providing limitless flexibility, these open-source architectures inherently introduce a level of complexity into the deployments. This can only be solved through the introduction of specialist Data Scientist resources/teams that can quickly spiral in terms of size and cost. These specialists are not only expensive, but they are also incredibly in demand, and the shortage of expertise in the IT sector is a well-known phenomenon that I'm sure I don't need to go into...

Alternatively, if the idea of toying with your Big Data platform at a system level doesn't appeal to your business, then there are a multitude of off-the-shelf products that could fit the bill. These tools are almost exclusively based on the Hadoop architecture, but claim to do all the heavy lifting so that you don't have to. Brilliant... in theory. In practice, these off-the-shelf products generally fall into one of two categories which have their own inherent challenges.

Firstly, there are those products which are locally hosted and built to customer specifications. Able to offer significant value to business of all sizes and solve challenges of various kinds, they come with one rather important caveat. I could, in theory, buy a Bugatti Chiron to solve my commuting problem, except I don't have a cool £2,400,000 sitting around to do so!

Secondly, the business could embrace cloud. Although I'm sure your business has already embraced cloud, judging by the sounds coming from the industry, every man and his dog has a cloud environment that is eating up whole swathes of compute within the major cloud providers' gigantic black boxes. However, if you're still in the process of dipping your toe in the proverbial shallow end of cloud adoption like a lot of other companies, then suddenly, sending all manner of data points to the cloud without considering all the potential security implications is naïve at best, and downright negligent at worst. Now that I think about it, that's probably the beginnings of an article unto itself...

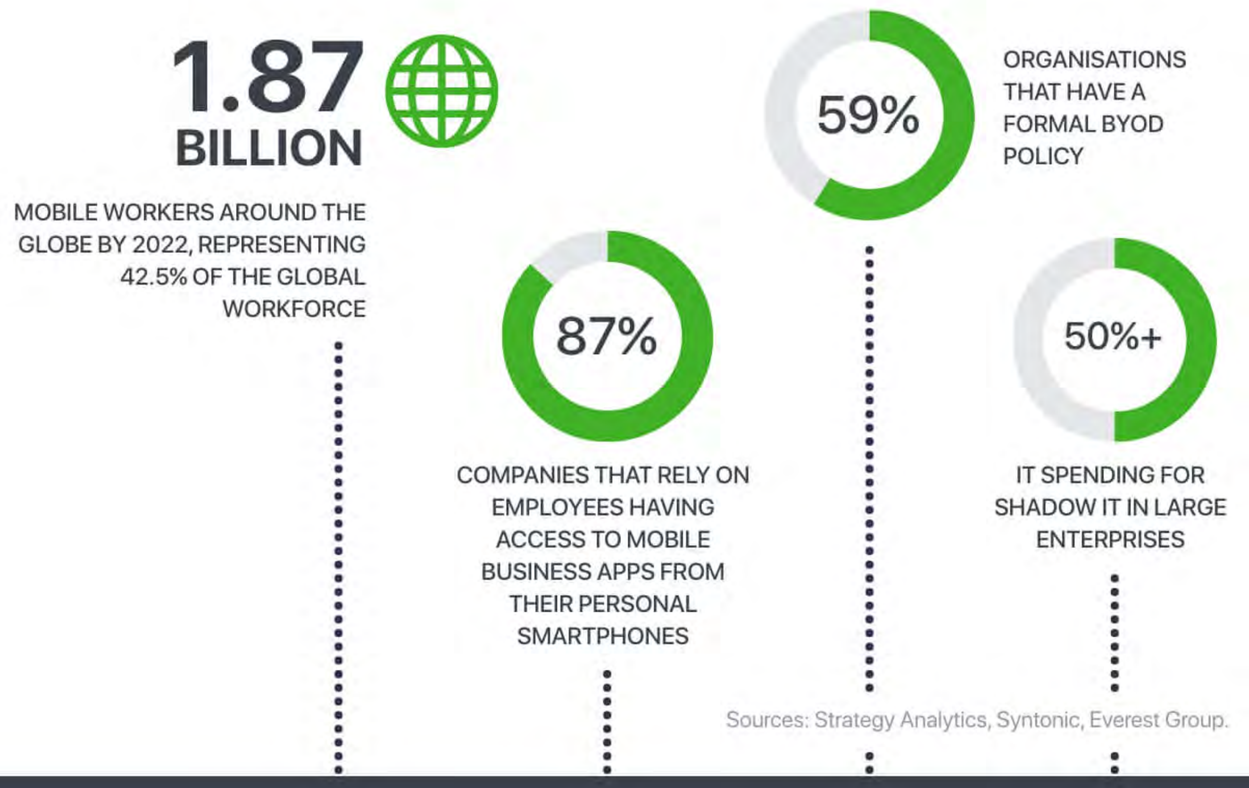
RETHINKING DATA SECURITY WITH A RISK-ADAPTIVE APPROACH

FORCEPOINT

The two megatrends of cloud-based applications and mobile devices have been a boon for company productivity, agility, and innovation. The mobile-cloud combo empowers employees to work and be productive literally anywhere. However, the mobile-cloud era has created a conundrum for cybersecurity teams. Here are some of the challenges:

If we look at how cybersecurity has traditionally been approached up to this point, it's centered on threat-centric responses. You built a wall around your perimeter, controlled access in and out of that wall, and when something bad happened, you responded. That was effectively your defense, and it was relatively easy to implement.

Today, the traditional perimeter has dissolved, primarily because of two changes within the enterprise: the rise of the mobile employee and the widescale adoption of cloud services. By the same token, cyber activity once easy to define as "good" or "bad" has become nebulous. This poses a crushing problem to threat-centric security, whose static policies are forced to make decisions about cyber activity with no insight into its broader context. The result is a disproportionate number of flagged activities, overwhelming security teams who have no way to understand the ones most worthy of investigation.



Today's Data Protection Options are Limiting

Today, IT security protects data in different ways, using a variety of different tools. These tools are designed to do the same thing—protect data—but none of them are really all that effective. That's because they use static, threat-centric policies to block or allow access to data. And that was OK when everyone worked within a perimeter. There are issues with siloed tools as well.

Traditional UEBA (Forensic Analysis): Learning why something happened yesterday does not stop the problem

Traditional Insider Threat (Constant Monitoring): Balancing workforce privacy and IP protection is critical

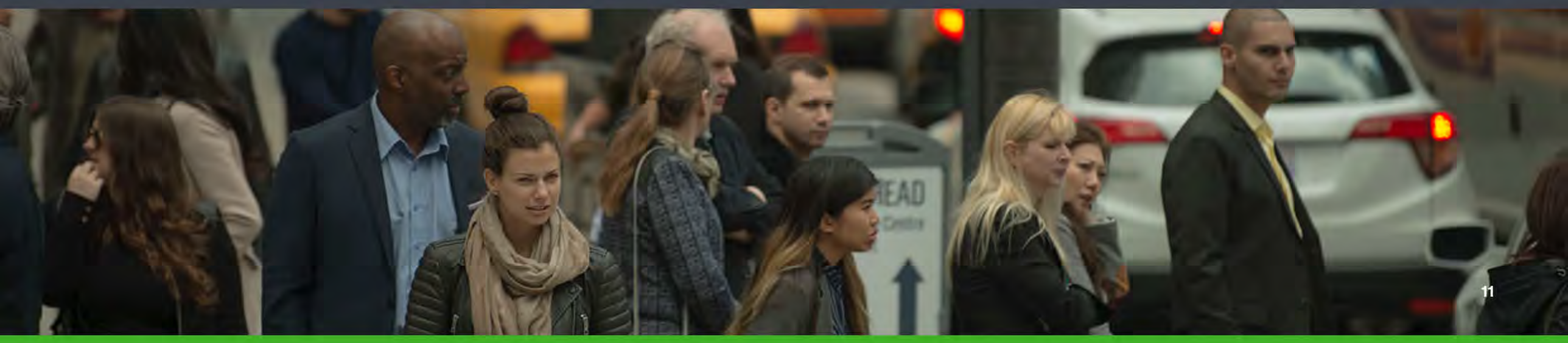
Traditional DLP (Block it or Allow it): Current policies are far too rigid to be effective

A New Paradigm

Instead of trying to extend the traditional, event-centric approach by adding more layers or crunching more data, we need a paradigm shift that places human behavior at the center of cybersecurity. Cybersecurity professionals need to focus on two constants—people and data—and where the two come together to conduct business. It's much easier to classify an action once you understand why someone took the action. This is at the core of increasing the efficacy of security organisations.

A Behaviour Centric approach detects individuals interacting with system that pose the greatest potential user risk, and will rapidly and anonymously understand potential risky behavior and context around it. This means an organisation can decide what is good or bad based on how users interact with your most valuable data, and so continuously revisit decisions as the organisation learns.

To learn more about how to take a Risk Adaptive Approach, download the complete eBook from Forcepoint at www.securityplusonline.co.uk.



Securing the Cloud:
The future of Authentication

The inexorable rise of digital connectivity and the ubiquity of devices is producing ever-increasing volumes of sensitive and personal data. For organisations, keeping that data secure, without affecting the productivity that is being driven by the digital revolution, is one of the biggest challenges for the IT department.

This transformation in how we access data at work has been built on an undoing of the traditional network - from the old network perimeter (and access via VPN) for a small number of users working at home. As this access extended to mobile and flexible workers, so authentication became an essential in helping to manage user security.

The Username-and-Password method as a secure access was widely replaced with VPN connections, and yet, as the number of applications which users accessed increased, it remained an essential part of the user experience, especially for on-premise applications. The assumption of local users being more secure meant that the inconvenience of authentication was rarely considered. To add, the move to the cloud has actually taken that assumption, rather than reverting to the best practice of an additional security layer.

> **It has been found that, on average, individuals have 26 different logins but only 5 different passwords.**
>
> Experian

So, is the cloud fully trusted? On top of this, how can a secure authentication model be translated to embrace the flexibility of cloud applications and the better user experience it offers? We reached out to hundreds of CIO, CISO and IT leaders to ask them about how authentication can bring the divide between security and productivity.

> **56% of CIOs were uncertain about their ability to enforce their security policies on a provider's site, while 45% were concerned about unauthorised access on what they deemed to be 'untrusted' networks.**
>
> IDG Cloud Computing Survey

It cannot be forgotten that public clouds are often just that - public. Those applications which are well known and accessible to anyone with an internet connection and credentials are still intrinsically tied to email addresses. When a password is the only defence against stolen credentials and unfettered access, it's time to re-evaluate the approach.

Usernames and Passwords have prevailed for a number of reasons, including convenience, speed of deployment, flexibility and cost. However, the biggest reason is perhaps user experience, as we all understand how this system works (no matter our own challenges in remembering long complex passwords that are unique to every site and application). Our technology ecosystem even drives this behaviour, not least browsers remembering passwords for us. The movement of traditionally consumer applications (such as Dropbox) into the corporate environment has also brought ease of use as a user expectation.

It's also often the product of shadow IT and BYOD; as departments increasingly purchase applications and services outside of the IT department and rogue devices consequentially appear (such as the CEO's iPhone), an all-encompassing approach to user identity management and security is very hard to apply.

swivelsecure

Some Highlights

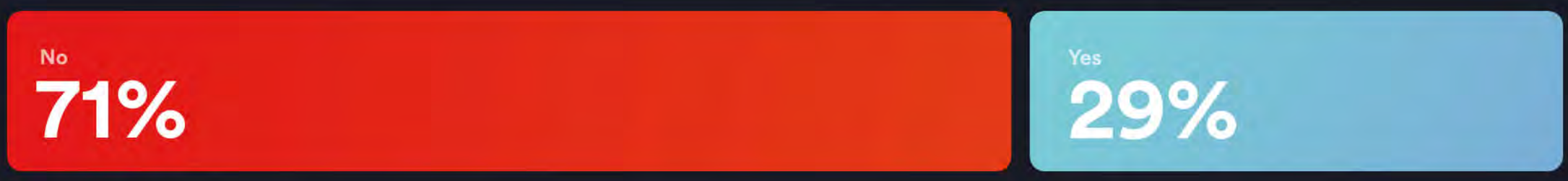
88%

Nearly 9 out of 10 organisations expect more use cases, in particular cloud apps

What do you use 2FA/Multi-Factor Authentication for?

For those organisations using authentication, the highest use case by far was for VPN/remote access. This has traditionally been the main driver for authentication, focused around securing the traditional network perimeter. However, not only are cloud applications now in second place, 88% of respondents see major growth in the next few years. Whether it's productivity apps such as Office365 or Dropbox for data storage, the importance of validating and securing access to data repositories is clear.

Do you offer users a choice (based on scenario – e.g. location, device being used, time zone)?



While offering users a choice was almost split 50/50, doing so in a dynamic way based on the specific use case scenario (such as the device used by the user, or what their location is) is significantly reduced - potentially reducing necessary security, or providing a frustrating user experience.

If you did deploy SSO, what would be the biggest reason?

SSO was identified as a clear priority - and respondents are clearly being driven by providing a better user experience, followed by improved security. Having a productive partnership with users on improving an organisation's cyber defences is a fundamental shift that's driving IT strategy.

To conclude, although it is clear that some organisations remain sceptical about adopting authentication across all applications and use-cases, user security and management is key to future IT strategy. The popularity of SSO and the increased implementation of technology that improves user engagement and productivity are key drivers, and will be part of policies that also improve user security and a more widespread adoption of authentication across the network and into the cloud. To read the full report visit www.securityplusonline.co.uk.

SECURING THE WHENEVER, WHEREVER WORKFORCE

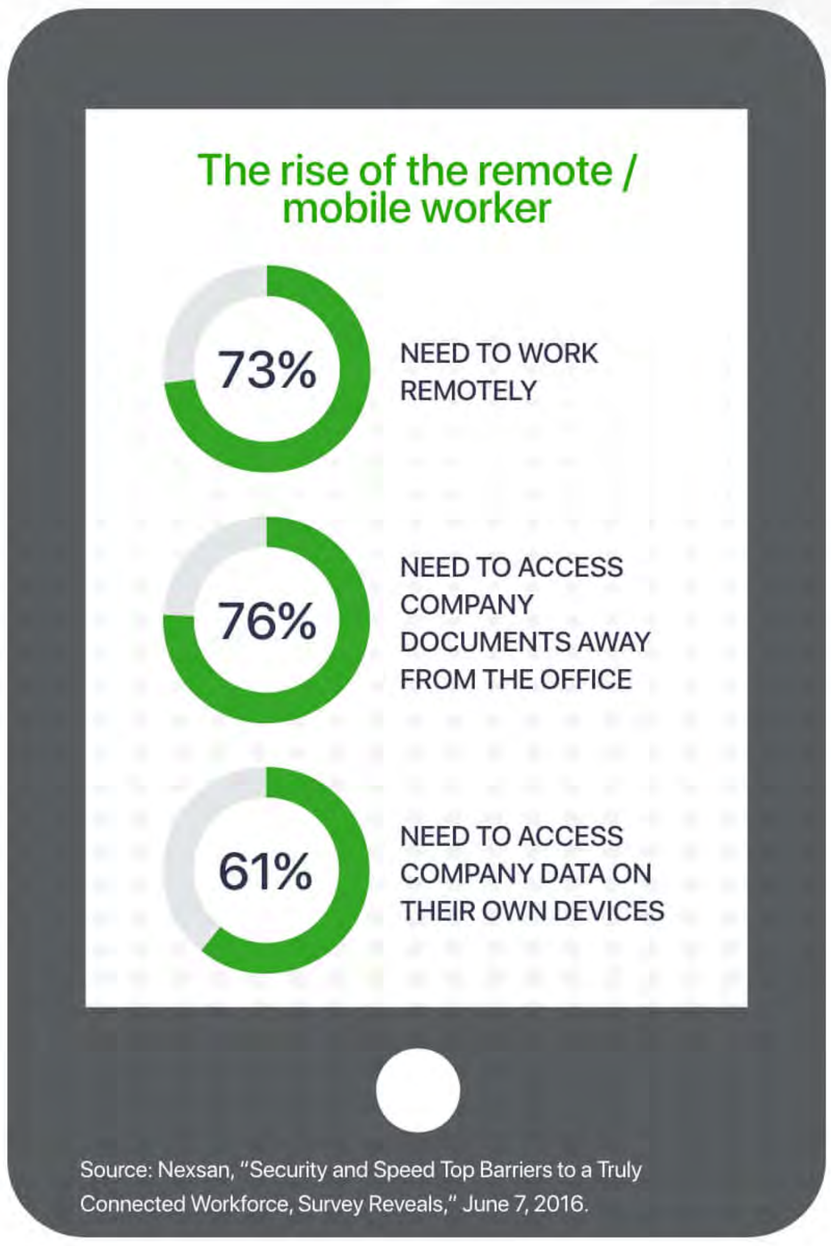
FORCEPOINT

Keeping up with the increasing security risk of the Mobile-Cloud Era

The two megatrends of cloud-based applications and mobile devices have been a boon for company productivity, agility, and innovation. The mobile-cloud combo empowers employees to work and be productive literally anywhere. However, the mobile-cloud era has created a conundrum for cybersecurity teams: how to secure mobile devices (particularly unmanaged bring-your-own devices [BYOD]) accessing cloud applications (which may or may not be sanctioned by IT) that store sensitive corporate data outside the control of traditional on-premises security solutions.

It's a challenge that grows more critical - and difficult - to surmount on a daily basis as various parts of the business continue to adopt software-as-a-service (SaaS) at an unprecedented rate. Security teams question how they can secure what their companies don't control or even own. How can they protect against both intentional and unintentional data leakage stemming from users accessing cloud applications from a variety of devices, including their own personal ones?

The short answer is to focus on securing people, protecting them from compromise as they use the cloud from any location, on any device. This guide highlights the security challenges and gaps in visibility that cybersecurity teams face and what they can do to mitigate the risk inherent in the mobile cloud world.



1.87 BILLION

MOBILE WORKERS AROUND THE GLOBE BY 2022, REPRESENTING 42.5% OF THE GLOBAL WORKFORCE

87%

COMPANIES THAT RELY ON EMPLOYEES HAVING ACCESS TO MOBILE BUSINESS APPS FROM THEIR PERSONAL SMARTPHONES

59%

ORGANISATIONS THAT HAVE A FORMAL BYOD POLICY

600 TO 1,000 SAAS APPS

USED AT A TYPICAL COMPANY

1/3

THE PORTION OF SUCCESSFUL ATTACKS EXPERIENCED BY ENTERPRISES THAT WILL TARGET THEIR SHADOW IT RESOURCES BY 2020

50%+

IT SPENDING FOR SHADOW IT IN LARGE ENTERPRISES

Sources: Strategy Analytics, Syntonic, Gartner, Everest Group.

THE SECURITY BLIND SPOTS INHERENT IN THE BYO WORLD

When the devices being used by employees are owned and managed by your company and the applications employees are using are hosted within your own datacenter, it's easier to provide adequate protection against cyberthreats. But let's face it, this scenario is starting to become an increasingly rare occurrence. The more likely situation today is trending towards a BYO-everything environment with employees or their business departments providing their own devices, internet access, applications, and more. This rise in mobile devices together with the growing use of cloud-based applications for everything from email to customer relationship management to financial reporting has given rise to a number of blind spots and security problem areas for security teams.

"*By 2018, the 60% of enterprises that implement appropriate cloud visibility and control tools will experience one-third fewer security failures.*"
Source: Gartner, "CASB Platforms Deliver the Best Features and Performance," 24th February, 2017.

WHY SECURITY FROM CLOUD AND CLOUD APPLICATION PROVIDERS ISN'T ENOUGH

Given the incredible uptake by companies of all sizes, you'd think that cloud and cloud application providers would be highly focused on providing security capabilities that address mobile/cloud application security blind spots. And to be clear, to some extent, they do provide capabilities that help.

However, security in the cloud is most often a shared responsibility. At the simplest level, the cloud provider is responsible for the security of the infrastructure while its customers are responsible for their data and user activities on top of that infrastructure. This means that security aspects such as user behavior, access and usage policies, and compliance are your organisation's responsibility. The same holds true for unmanaged devices. Cloud application providers generally don't distinguish between managed and unmanaged devices, nor do they provide compensating endpoint control capabilities. It's up to your company to secure access to cloud applications by both managed and unmanaged devices, as well as protect users and data, and detect and prevent cyberthreats.

> **By 2018, 40% of Office 365 deployments will rely on third-party tools to fill in gaps in security and compliance, which is a major increase from fewer than 10% in 2015.**
>
> Gartner, "CASB Platforms Deliver the Best Features and Performance," 24th February, 2017.

SECURITY STARTS WITH YOUR MOBILE WORKERS

Every security team knows that network perimeter defenses and endpoint protection aren't the answers when it comes to securing mobile workers. After all, employees today rely on a dizzying combination of sanctioned and unsanctioned cloud applications and managed and unmanaged devices.

So what is the answer? It's focusing on the one common denominator across all the scenarios: the human. Visibility into user and entity behavior must become the focal point of your security efforts.

Insight into usage patterns and device profiles enable proactive policy enforcement and account protections across managed and unmanaged endpoints. This insight gives you a way to surface and respond to abnormal user activity to protect both your users and data in the cloud.

How to Build a Security-Centric Culture in Your Company

When almost any business relies on stable and secure IT operations, cyber security is not something just IT staff must care about. A forward-thinking business leader should manage cyber risks on an equal footing with all other business risks. It was even recognised on the World Economic Forum this year: for the first time in history, the forum's Global Risk Report claimed that cyber risks – cyberattacks and breaches resulting in data theft or fraud – are among the chief threats to businesses.

Moreover, if you look at the Verizon Data Breach Investigations Report 2018, you see that employees with legitimate access rights are the second most frequent reason of a breach: either because of human error or an attack, since attackers usually look for the soft underbelly like trusting insiders.

To ensure that cyber risks are addressed correctly in your company, you should achieve a shift in the employees' mindset – this can be done by building a culture that values cyber security. In this article, I will explain what steps to take to start establishing an effective security-centric culture and what benefits your business will get.

Step 1. Identify zones of responsibility

Since all big shifts in the company's course start at the senior level, it is important to employ "leadership-driven cyber governance". The leader's role is to articulate mission statements on why the business has to take security seriously and highlight how it contributes to the company's growth. If employees know that the corporate leadership is actively governing and nurturing cyber security and that it is a cultural priority, they will be less likely to oppose the change.

Cyber security is an organisation-wide issue, so the incorporation of a security-centric culture should be a joint effort. Firstly, I would recommend appointing a board member, such as the CIO or CISO, to regularly report on cyber security to the rest of the board: How well the company is prepared for incidents and how business will benefit from further investments in cybersecurity. IT security teams cannot afford to stay siloed anymore.

However, IT security is not only about IT staff. Mid-management who work with business users directly also play a big part, since they can control how their subordinates follow the policies. On top of that, HR staff should communicate the new culture to the employees and oversee training. While Legal is responsible for ensuring that cultural statements align with compliance regulations and with national and international legislation.

Zones of responsibility may vary, but the key to success is all the same – effective delegation and joint commitment.

Step 2. Clearly document security policies

A security policy is a guideline for employees and the cornerstone of your security-centric culture. To communicate it, your teams should come up with two documents. The first one is the official security policy prepared by IT that each employee has to sign off on. It identifies rules and procedures everyone accessing the company's systems and using its IT assets must follow.

The other is an informal document composed by HR aimed to explain the company's vision towards security and highlight why following security best practices matters for the growth of the business and to every employee. In our company, we have the security section in the employee handbook, which each newcomer reads on the first day.

Step 3. Train employees

Cyber security training may seem labor-intensive but it is efficient in fostering a security-centric culture. According to Netwrix 2017 IT Risks Report, 37% of respondents claimed insufficient staff training as one of the major obstacles to implementing a more efficient IT risk strategy.

Training may take the form of presentations, role-playing games and so on – format and frequency are up to the company. I would only recommend ensuring that training content differs depending on the employees' level of responsibility and knowledge.

In our company, every newcomer has to go through a video training on security and sign off that he did it before getting to work. We noticed that employees that attend such training almost never have problems, while before people often called the helpdesk for the basic stuff.

I would also advise paying attention to social engineering. If email security solutions were a catch all, I doubt the half a billion users globally who were targeted by massive phishing attack in the first quarter of 2018 would have been caught out. The best way to raise awareness is to conduct simulations of phishing attacks, so the IT team can pinpoint employees who tend to trust malicious emails, teach them to identify phishing, and explain their further actions.

Step 4. Encourage people to report on incidents

If you imagine that your company is the state, employees are the citizens that contribute to its prosperity if they are socially responsible. To nurture "security responsibility" in your company, mid-management should encourage subordinates to report on incidents or suspicious things they encounter, and provide an easy way to do it. Normally, reaching out to the IT staff directly suffices. Thus, the IT team will know if malefactors are targeting the company and will be able to react faster.

It is great if a manager can highlight his team member who helped detect a problem - in an email or a corporate meeting - to encourage others to do the same and claim victory together.

Step 5. Celebrate success with your new culture

In the long term, deep security awareness will become your additional layer of defense to prevent data breaches and thwart cyberattacks, the impact of which is estimated in billions of dollars and irreversible reputational damage. Building a cyber security culture does not require much financial investment but it does need a lot of willingness.

I also expect the security-centric approach to running a business to become a new trend. With the number of breaches rising and cyber threats becoming nastier, such an approach is not empty rhetoric but the only possible way of doing business right. The companies that manage to develop a mature cyber security culture will be valued more than ever.

“Cyber security is now part of the fabric of day to day life for us all, there is a huge opportunity for businesses that understand it, and use the new paradigm as a business enabler.”

Matt Middleton-Leal
General Manager EMEA at Netwrix

riverbed

5 Tips to Avoid Public Wi-Fi Security Dangers

Public networks in cafes, airports, train stations and in the workplace are undoubtedly convenient for all of us. Especially when we are abroad and want to avoid roaming bills or are running out of the monthly data volume, we rely on Wi-Fi hotspots. With just a few clicks we can connect to a fast internet connection, most often free of charge.

Many providers do not use encryption security. Encryption transforms all the information you use online into a code that is inaccessible for others and therefore ensures that your personal data are secure. A device that is connected to an open network can be hacked within less than two seconds without you even realising it.

There is a risk that a hotspot was set up by a criminal, mimicking to be a public secure one. Most commonly, in locations where public Wi-Fi is expected, near popular tourist spots, these rogue networks are installed. Fake Wi-Fi hotspots use harmless names like “Free Wi-Fi” and can be used to collect your personal data and information. These can be details of your bank records, passwords as well as emails.

A ‘man-in-the-middle’ attack can occur when a hacker intercepts data exchanges. The attacker captures and additionally manipulates information in real-time. Security lacks in applications, websites and networks are exploited to see all the information that is transmitted. Unencrypted Wi-Fi hotspots serve as an optimal access point for hackers to position themselves between your device and the network.

But you can protect yourself while being connected to a public Wi-Fi hotspot.

Enable your firewall: Ensure that your device is protected with a strong firewall to help avoid potential security threats from other users on the network. Keep your software up-to-date to have the latest virus protection.

Use a Virtual Private Network (VPN): This will encrypt and anonymise all the traffic. Attackers can only see that there is a connection to a VPN server but are not able to monitor which data are send using that network. Simply download a VPN application on your device and turn it on as soon as you connect to a public network.

Be vigilant: Before connecting to a public Wi-Fi hotspot you should read their terms and conditions in case they have these. Additionally, make sure to only submit information on websites that start with HTTPS instead of HTTP. This signifies a secure site that encrypts the transmitted data and your information has a greater degree of safety.

Browse with caution: Generally, you should avoid accessing websites that ask for sensitive data like passwords, credit card or account numbers. If that is unavoidable, log out from personal accounts as soon as you are done, so you are no longer subject to exposure.

Turn Wi-Fi off when not in use: Even when you are not connected to a Wi-Fi hotspot, your laptop or smartphone is still sending data to and from any network within a certain range. To avoid that your device connects automatically to hotspots you may have used in the past, turn automatic connections off in your settings.

There is a way you can use public hotspots safely without downloading any application. Riverbed Xirrus EasyPass combines security and simplicity, allowing guest, visitors and employees to automatically and easily create their own secure personal Wi-Fi network on public Wi-Fi. It safeguards users and their data when accessing public Wi-Fi, guest networks and hotspot environments.

Safeguarding – Your moral duty of care?

There are lots of different reasons why you might need to consider safeguarding, but how does it affect your organisation, what are your obligations ? It could be mandated via industry guidance, regulation or legislation. Maybe it's more moralistic or driven by social responsibility. Whatever the motivations are, it can be a difficult subject to tackle. Especially in cyberspace, with often very technically adept individuals as the subjects of your safeguarding responsibilities.

What is Safeguarding?

Essentially it is preventing and protecting individuals in your care, or potentially employment, from exposure to materials that may cause themselves or other individuals to come to harm; either mentally or physically.

What does it mean for IT?

From an IT security perspective, we may think that by blocking access to particular material online it's enough. in reality, if someone really wants to access the information they will typically find a way. However, if that's not through the organisational network or through supplied devices then it's not your concern – right?

It could be argued you have taken all the steps you could to stop access to that information. Therefore if something happens outside of your organisation relating to that individual successfully accessing and then acting upon the information, you may well be right in thinking you did all you could....

Morally, is this where we as IT professionals, teachers, governors should draw the line and say we did enough? When we consider where that line is, what is driving that decision? Is it purely philanthropic?

With the right tools in place, and a clear understanding of the safeguarding aims, we can do a little more than just the bare minimum. Monitoring of individual's online data is always undertaken with trepidation, but is it the monitoring of that individual's activity and balancing that with their right to privacy that should concern us, or the ways this could potentially restrict academic endeavour, discussion and debate of controversial topics.

In order to get the balance right we need to have grown up discussions, understand who we are safeguarding and what are the dangers we need to be looking out for. Do we want to restrict access to researchers or teachers looking up information on controversial topics? No. But we might want to stop and be aware of people accessing that information for other reasons. Where possible we need to understand what that individuals motivations for accessing that information might be, using this information to define our policies and actions. What is acceptable for our own organisational functions and roles.

Part of how we can achieve this is through leveraging the power of Big Data Analytics and Machine Learning. Correlating what the activity is with what we might know about that individual.

We know someone accessing self-harm forums could be a potential flag, but what is the context? By understanding who that individual is, are they the welfare officer or are they a student, we provide context. Adding other key metrics like how many times have they tried to access that type of information, what key words are they searching for, we can make informed decision – quickly and efficiently.

With the power to view this context comes responsibility. We need to make sure that this data is only accessed by the relevant individuals, the people who can react, such as those responsible for safeguarding. These individuals rarely sit within the IT function, so we need to have the tools that allow IT to become facilitators of information without having access to the specific data. Only then can we really start to tackle the challenge of safeguarding.

Contact us at LogPoint to find out more about how we can help you confidentially monitor, report and conform to your safeguarding requirements.

Connecting the Internet of Things

NETSCOUT™

The Internet of Things (IoT) can be daunting to understand considering the overwhelming amount of articles available on the subject. Meanwhile, the rapid proliferation of new IoT devices continues in both our personal lives as well as in virtually every industry. The purpose of this document is to quell the hype and facilitate a discussion of how to prepare for and manage an IoT deployment at a fundamental level.

This document will provide some best practices to help you understand how to deploy, validate and troubleshoot using purpose-built solutions that are designed to be quick and easy to use, such that anyone on the IT team of any skill level can become proficient at these tasks, allowing organisations to do more with the available staff.

The Drive for IoT

Digital transformation is driving a rapid proliferation of IoT devices, which will require IP connectivity and – in many cases – network-delivered power. Organisations are moving towards more IoT connected devices in an effort to drive down operational costs, and upgrade building automation systems to achieve efficiency gains, such as in HVAC and lighting as just two examples. This move compels integration and cooperation across IT, and OT (Operational Technology) organisations and technologies. This puts increasing demands on already-strained enterprise access networks and support resources. The image below provides an example as to the breadth of the types of devices that are becoming network connected.

Other devices may be connected via a PAN (Personal Area Network) with technologies such as wireless ZigBee, Bluetooth or the new Bluetooth 5 developed with IoT in mind. These PAN devices are usually connected to the networks via some kind of Field Gateway which is connected to the Ethernet network. There are other connectivity technologies – such as cellular technologies 3G, 4G and in the future 5G – for connecting IoT devices but the majority of devices, currently an estimated 10 billion, are connected in some way to an Ethernet 802.3 wired or 802.11 wireless connection. Connecting IoT devices or machines to each other and other control systems requires the skills of a highly-skilled network engineer. However, using the right tools that are designed to be used by any skill level through automated tests and pre-configured profiles will ensure an effective deployment as well as ongoing support and troubleshooting.

Strategies to Ensure a Successful Deployment

It is important to understand the challenges of deployment that can occur not only across organisational silos, but also those that are likely to occur when outside vendors are involved. As noted earlier in this document, some types of devices you may be deploying would be typically part of the operational technology (OT, or facilities) group, such as lighting, access controls, and HVAC.

However, since these systems will now become network-connected and likely require Power over Ethernet (PoE) for power, facilitating collaboration between IT, OT and any third-party vendors should be a principle component in your deployment strategy. You can imagine that between all the various groups involved, each may only have a perspective of their specific component, which could mean finger-pointing should problems arise. This can become frustrating, time-consuming and expensive, so advanced planning and communications are key to lessen or eliminate the finger pointing.

IoT Device Configuration

During both the deployment and ongoing support, you should have an understanding as to how your devices are configured and managed, even if a third party will be doing the initial install. Today, most device vendors have either an Android™ app-based, or cloud-based application to facilitate device configuration. You should familiarize yourself with what is available for the devices being deployed and by whom, and how those applications will be accessed during deployment as well as ongoing support and troubleshooting. This will help you to identify both resource responsibilities at the various project phases, and what tools and connectivity methods are required.

Planning Considerations

During the planning phase, you should take into consideration both local and remote site needs with regard to IT support, device configuration, network connectivity testing requirements and performance, plus the need for documentation.

Identify IT Resources

Give some thought to the resources you have available to help with deployment as well as on-going support. As you think about these resources, consider how enabling more individuals could help to offload deployment and troubleshooting tasks from more senior technicians or network engineering. Senior network engineers are typically frustrated by the volume of escalations that distract them from important IT projects. Through use of the right toolset, many organisations are finding success in enabling lower-level technicians to find more problems on their own or provide them with the ability to escalate more effectively with actionable visibility. This alleviates workload from network engineering, improves collaboration, and enables teams to be more efficient with the same staffing resources.

Network Connectivity Requirements

Every deployment and network environment will have its own set of unique network connectivity requirements. Spending time up front to identify what these parameters are will save time and frustration down the road by having a standardised and agreed upon network connectivity requirement. As part of defining this requirement, you should establish a plan for both how it will be validated and who will do the validation. You will want to find a way to run the required set of tests in an automated, consistent way that allows a broader team to help spread the workload across more people, regardless of their skill level. An example of validation parameters would include:

- **Required PoE voltage level at the connection jack**
- **Speed/duplex**
- **Switch detail, such name slot/port/VLAN**
- **Internet connectivity address/port**

Documentation Needs

Documentation of connection path between jack and switch slot/port/VLAN as well as other parameters, such as information about the connected devices is desired, but not always easy to obtain and maintain. Documentation is also essential for when problems arise down the road. Having a baseline of what things looked like when everything was working and connected properly saves significant time when troubleshooting. Define what information would be useful to your organisation to have along with how it should be organised, be it by site, floor or other. Also, identify who will need access to this information during both the initial input of information as well as down the road when it would be useful in troubleshooting.

Avoiding Finger-Pointing

There may be many departments and outside contractors involved with the installation and ongoing maintenance of IoT devices and systems. Therefore, it is imperative that all involved come together under one project to assess, identify, and agree on the connectivity requirements for the deployment, as well as access to device configuration resources be it on premises, in the cloud, or Android™ app-based[1]. This ensures that all parties understand the requirements for the deployment and what performance is expected of the device for ongoing maintenance and troubleshooting. Once the network and services requirements are completed, a set of network connectivity tests and reporting requirements for validating the installation, together with an ongoing support strategy and ownership, should be specified.

Qualifying Network Services

When organisations deploy or troubleshoot IoT devices, the most fundamental component is the ability to ensure the network services required to support the connected device are configured and working correctly. Network services would include link speed/duplex, PoE, switch configuration, IP address assignment, DNS and Gateway connectivity and connectivity to required resources.

By having an automated method to perform each test the same way every time, organisations can not only ensure a consistent and repeatable testing process, but should a problem occur, the automated test will provide an indication of the problem domain. When an escalation to network engineering is needed, problem triage can begin faster with actionable visibility into problem domain. It helps knowing what tests were already run by the technician so time is not wasted performing the same tests, so more advanced troubleshooting can begin right at the core of the issue.

The Right Tool for the Job

When identifying the test parameters necessary to validate IoT device deployment, it is important to consider the test equipment that will be able to meet your needs. The most important factor is to ensure a consistent, repeatable set of tests (i.e. an AutoTest), which ensures the same tests with the same test limits can be initiated by all technicians throughout the deployment project. This, along with the ability to obtain test records in an automated way to a central database of measurement results, will provide not only a platform for collaboration and reporting but also a baseline of correct connectivity, useful for future troubleshooting. This central view of results could identify a common component or service failure very quickly, therefore averting a major project delay or major expense. This also facilitates ongoing support after the devices have been installed and commissioned. This could be local or remote support allowing more experienced engineers to collaborate and help resolve problems faster by using the tester's remote visibility via the cloud service or real-time control over the network.

Consider different tool requirements based on skill level of user, varying requirements by site, and of course budget to find the solution mix that's right for your organisation. Having the right solution can also prove useful should finger-pointing occur, by being able to identify if a given problem is in the network or the device itself.

Conclusion

The proliferation of IoT connected devices in today's network environment is challenging organisations to do more with the same staff. It also creates the potential for increased complexity of project management across organisational silos and outside vendors. Therefore, as you embark on managing and supporting the deployment of more and more network connected devices, give some thought to how you can expand your ability to manage the project by enabling more resources, build collaboration across teams, and ensure you have the visibility you need to control the finger pointing when it begins.

1 Android is a registered trademark of Google Inc.

The Forgotten Hero – Patching

How often do your employees carry out regular maintenance / updates to their 'computers'? When should they do it? (or should IT expected to perform such tasks?) Reminding employees to carry out important computer maintenance usually falls by the wayside, so the responsibility then falls upon the business to make sure that they are conducting basic IT health checks.

In fact, companies should take notice of this now more than ever as the cybercrime threat becomes increasingly dangerous. Not only did we see a huge amount of high profile hacks last year, including those which utilised weaponised malware, such as WannaCry and NotPetya, but according to recent research by the Online Trust Alliance, 160,000 cybersecurity incidents were reported in 2017, nearly double the 82,000 incidents that were reported in 2016. So far this year, multiple forms of new and manipulated malware have appeared, posing new threats to businesses. For example, Scarabey, a new version of the old Scarab ransomware, has surfaced. The bug threatens to delete 24 files every 24 hours until a ransom is paid in Bitcoin.

The dire state of the security landscape means that businesses need to make sure they are taking cybersecurity seriously and making sure they implement necessary measures effectively.

Getting Back to the Unsung Basics

As organisations look to strengthen their cybersecurity statures in 2018, I recommend that they look to implement the basic security best practices that National Clean Up Your Computer Day looks to promote, beyond simplistic practices like wiping your computer screen down. While some businesses may have taken certain strides towards increased endpoint security in the wake of 2017's devastating attacks by patching quickly and comprehensively, and demonstrating compliance with company policies, this still isn't a priority for many companies. The OTA report mentioned above revealed that 93% of reported incidents could have been prevented by following basic security best practices, such as implementing patching software.

All too often, organisations invest too much of their security budgets on a wide range of solutions that aren't compatible as a whole, and don't provide teams with a comprehensive picture of the risk environment. In many cases, this actually results in gaps being created as organisations juggle multiple vendors and solutions. A layered approach to cybersecurity is necessary in order to best protect against attacks, so organisations should cater for the basics as well as using more complicated solutions. So, while the humble patch may seem simple, it is arguably the forgotten hero that needs to be celebrated, and certainly implemented, on National Clean Up Your Computer Day.

Software is Inherently Vulnerable

Patching is essential for the very simple reason that software is inherently vulnerable. It is easy to forget in this digital age that the hundreds of thousands of lines of code out there are all written by humans. Unfortunately, people aren't perfect and often make mistakes, which means that no software is completely free of all errors or immune to cyberattacks. Furthermore, as software ages the more likely it is that vulnerabilities will be exposed and thus become vulnerable to exploitation.

WannaCry illustrated that a lot of known vulnerabilities don't get patched. Patching was available for supported Windows operating systems before and after WannaCry hit and Microsoft pushed an emergency patch for unsupported versions including XP, Vista, Windows 8, and Server 2003 and 2008 Editions. Despite this, it appeared organisations didn't learn their lesson as a month later thousands of organisations globally became victims of the NotPetya attack, which also exploited vulnerabilities which had existing patches.

IT health checks are crucial - just because a patch is available doesn't always mean that it is being implemented correctly and this needs to change within all organisations. And with the annual average cost of cyberattacks per business valued at $11.7 million in 2017, organisations can't afford not to carry out basic security maintenance that ensures that patches are being implemented properly.

Automation Can Lighten the Load

An unpatched hole is like an open window or an unlocked door to a hacker. This raises an important question: if patching is so essential, why did 93% of organisations who reported a security incident fail to properly implement cybersecurity basics last year? The problem with patching is that it is a long, wearisome process when done manually. Furthermore, organisations often forget that that programs and data hosted on virtual servers and in the cloud need to be patched, as well as physical devices. There is certainly a lot to think about to ensure that the job gets done correctly.

This is why I suggest that organisations should look into automating their patching. This would ensure that systems are continuously scanned for missing patches and automated solutions can deploy patches where necessary and without human intervention. Cybersecurity teams would therefore have more time to dedicate to more proactive tasks, and can receive real-time reporting in order to remain informed, and compliant with the upcoming GDPR and NIS regulations which require full visibility into an organisation's systems.

So, its time to seize the opportunity to remind your employees to perform basic maintenance on their computers, for example make sure that unused and duplicated files and programs are deleted. But, even more importantly, I just want to hit home that you should take this opportunity to ensure that your cybersecurity basics are being implemented properly within your organisation to ensure that internal security is strong from the ground up.

Chris Goettl, Director of Product Management, Security at Ivanti
Image Credit: Sergey Nivens / Shutterstock

Take the time to update and patch your system…

ivanti

SECURITY+

Visit **www.securityplusonline.co.uk** for the digital quarterly updated version of the magazine

e92plus

+44 (0)20 8274 7000

@e92plus

/company/e92plus

www.e92plus.com

info@e92plus.com

Featuring Vendors

ivanti FORCEPOINT TREND MICRO netwrix LOGPOINT

NETSCOUT Cyber Risk Aware Creating your human firewall! swivelsecure riverbed