Cybersecurity eBook
June 2018

BUILDING A BETTER APPROACH TO FEDERAL CYBERSECURITY

Protecting Federal Networks with the most Advanced Defensive Tools

CONTENTS

CHAPTER 1

Building A Better Approach to Federal Cybersecurity

No two federal agencies have the exact same cybersecurity layout, yet all of them are bristling with layered defenses to try and keep attackers at bay. Between firewalls, security operations centers, endpoint protection, traffic scanning, analysts on duty 24-hours a day, event logging, honeypot deployment, anti-virus, behavioral analysis, geofencing and hundreds of other tools and tactics, it would seem on paper that most federal agencies should be completely secure.

However, all those complex defenses have proven ineffective time and time again, especially when faced with the type of threat actors, such as those funded and employed by rival nation states, that constantly target the federal government. According to a recent security study, government was the fourth most popular hacking target in 2016, following healthcare, manufacturing, and financial services.

And unfortunately, many recent attacks aimed at government have been wildly successful, even against agencies with extremely robust security. Last year, the contact information for over 20,000 FBI employees was stolen off agency computers and later published online. And in November, the personal data for more than 130,000 Navy workers were taken by hackers. The largest hack to date included the theft of sensitive personal data in history at the Office of Personnel Management ("OPM"). As was noted in this attack and in virtually every other, is the lack of ability to detect, mitigate and respond to such threats due to an apparent reliance on outdated and ineffective methods and lack planning for the evolving methods.

While traditional security can stop hundreds or thousands of attacks every day, it's never been perfect. Clearly, the continued buildup of complex security devices, programs and defensive tactics has not been completely

> "That feat is not magic, and the technology is available."

successful for some of our most important organizations. In some cases, attackers have been able to use that complexity, and the many false positives such a burden-some system produces, to hide their movements and mask their true intentions.

Beyond the complexity problems with layered, traditional security, is a key factor that limits its ability to successfully stop all attacks. One hundred percent of cybersecurity programs today rely on legacy IP and Multiprotocol Label Switching (MPLS) backbones. So do all the routers, switches, servers, clients and other equipment that make up every network. Attackers obviously know this, and use it to their advantage to recon networks and plan their post-breach lateral movements. Static IP addresses coupled with the complexity of cybersecurity defenses gives attackers a tremendous advantage over beleaguered defenders.

But what if there was a better way? What if an entire network could be lifted off the burden of IP dependence with one quick installation? Whole networks would seemingly "disappear" from a hacker's radar, leaving them unable to find any assets to strike at, and making it impossible for them to search for preferred targets and data. A technique that could perform that seemingly impossible trick would also wipe out the need for overly burdensome cybersecurity defenses, making networks untouchable to unauthorized users and eliminating the need for such defensive complexity.

That feat is not magic, and the technology is available. It's called Identity Defined Networking, and when deployed using an approach pioneered by IMPRES Technology Solutions, it can lock down and protect networks in a way that attackers can't overcome.

ADVANCING BEYOND IP NETWORKS

The key to the revolutionary new IMPRES approach is removing IP identifiers from all devices across a network. This is not unlike a NATing process, except instead of simply assigning internal devices a new IP address, which is still discoverable from the outside, IP is completely removed from the picture. The goal is simplicity, scalability, and ease of use. With Identity Defined Networking (IDN), each device instead receives a unique host identifier in the form of a long-lived CryptoID. From that point, devices on the internal network will only respond to traffic from explicitly whitelisted systems or endpoints coming in through encrypted channels. Designed as a seamless and non-disruptive network overlay to existing infrastructure, the standards-based architecture supports all legacy and modern resources regardless of environment. This allows organizations to reduce errors, minimize address-based rule sets, and reduce complex point solutions.

Now, any organization can instantly connect, cloak, encrypt, micro-segment, move, revoke or failover any networked resource, anytime, anywhere – simply, cost effectively

and safe from hackers and human error.

Devices will now use their unique identifier to talk with one another, completely ignoring IP. Any attempt to use IP to find devices on a protected network will fail, as will any hacking, discovery or probing tools that depend on IP. In addition, any unencrypted traffic will be dropped.

The use of IDN completely strips attackers of their ability to infiltrate a network, or to move laterally should any endpoint somehow become compromised. And, the IMPRES approach uses a fabric-based architecture that integrates networking and security into a unified platform that works with all topologies, protocols and hypervisors. It also works with any mix of wired Ethernet, cellular, Wi-Fi, or SatCom networks, so is completely platform agnostic.

INSTALLING IDENTITY DEFINED NETWORKING

For such a huge advance in networking, installing IDN is a relatively effortless process. The brains of the IMPRES approach runs off a 1U Dell EMC rack-mounted server, the only hardware the solution requires. Called a Conductor unit when used with IDN, it is responsible for removing IP from an internal network and replacing those numbers with encrypted host identifiers. Even on very large networks, the typical installation time for the transition is often under an hour.

As part of that install process, agents are placed on devices to enable them to drop their IP addresses and work with the new system. Most devices can accept the agents, including those such as medical equipment or unmanned aerial vehicles that can be targeted by attackers, but which do not have traditional user interfaces. Once they move to IDN, they are cloaked and hidden from attackers just like desktops and servers. Even tiny devices such as those that are part of the Internet of Things can be protected with IDN. If an agent can't be directly installed, a software solution can sit above the device in the network, protecting it as effectively as an internal agent.

For users working on a network after IDN is installed, nothing will change. They will be whitelisted as part of the installation process, so everything they have always used will still be available to them in the exact same way as before.

For the IT staff, very little will change. The main difference is that to make network changes they will need to first log into the Conductor. Thereafter, they can do what they always have without the need for additional training.

EXPLORING THE IMPRES APPROACH

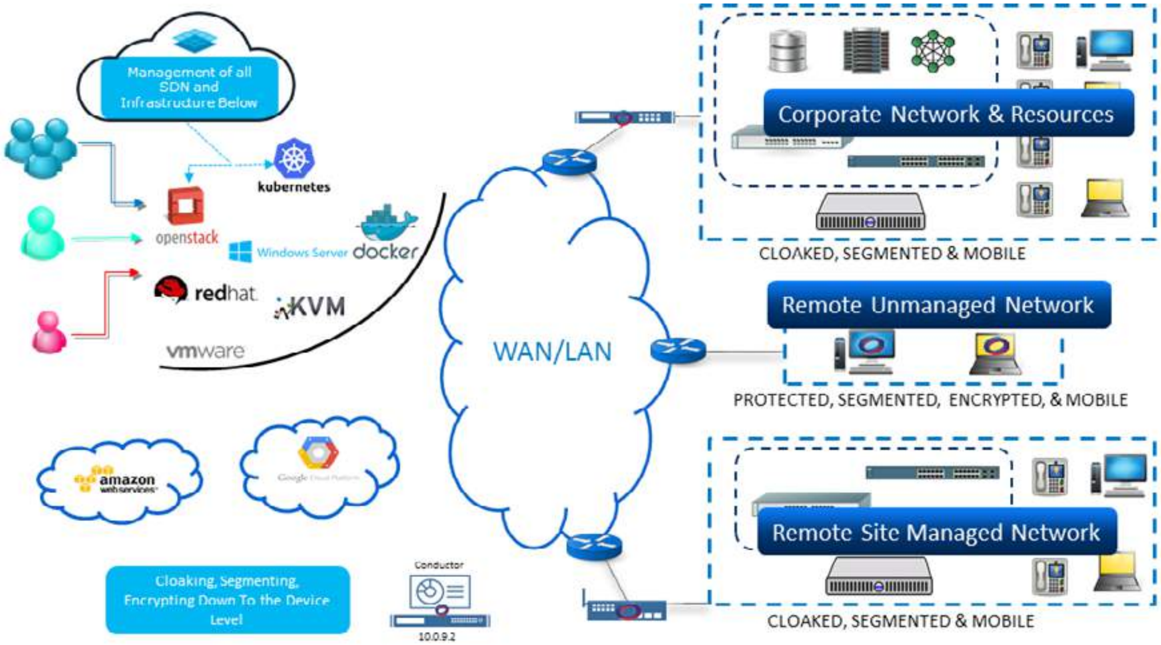
It's clear that moving to IDN can reduce both the attack surface and cybersecurity complexity for

//IMPRES Technology is dedicated to assisting our federal customers overcome technological and architectural shortcomings without selling golden hammers”

federal networks. With IDN at the core, the IMPRES approach can improve security and efficiency for agencies in several key areas including cloud computing, performance analytics and situation migration, collaboration and end-point protection.

“IMPRES Technology is dedicated to assisting our federal customers overcome technological and architectural shortcomings without selling golden hammers,” said IMPRES Technology Solutions Executive Vice President Steve Ridgeway. “The United States is under continuous attack and probing by nation states and rogue individual actors. We want to do our part to assist in protecting our nation’s most valuable assets for future generations.”

In the next chapters of this eBook, we will cover how to protect those critical assets in more detail, expanding on the benefits that can be achieved by using IDN and the pioneering IMPRES approach to improving federal networking.



Management of all SDN and Infrastructure Below
kubernetes
openstack
Windows Server
docker
redhat
KVM
vmware
amazon web services
Google Cloud Platform
Cloaking, Segmenting, Encrypting Down To the Device Level
Conductor
10.0.9.2
WAN/LAN
Corporate Network & Resources
CLOAKED, SEGMENTED & MOBILE
Remote Unmanaged Network
PROTECTED, SEGMENTED, ENCRYPTED, & MOBILE
Remote Site Managed Network
CLOAKED, SEGMENTED & MOBILE

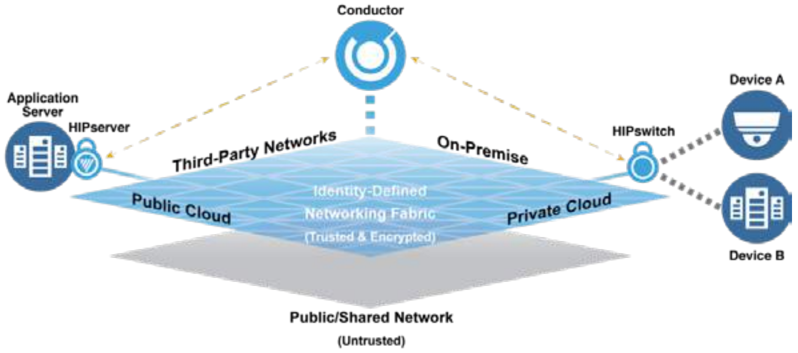
CHAPTER 2

Achieving Secure Cloud Computing with IMPRES

FEDS TIPTOE INTO THE CLOUDS

Organizations across all industries are moving away from their reliance on physical infrastructure into the promise of cloud computing. With its many performance, scalability and economic benefits, especially over time, cloud applications can be extremely attractive compared to constantly having to upgrade physical servers and network infrastructures. Most cloud deployments are owned by a cloud provider, so all the work to maintain it falls on them, with customers only responsible for paying a user fee. And that fee is dependent on usage and capacity, so users can pay as they go, and only for what they need.

In the federal government, the prospect of moving to the cloud has been especially attractive, especially in the wake of programs like the Federal Data Center Consolidation Initiative (FDCCI), which was created in 2010 to reverse the historic growth of federal data centers, or the Data Center Optimization Initiative (DCOI) which replaced it, but with similar goals. In the federal space, physical data centers were growing out of control, with thousands popping up across agencies, and with many performing overlapping functions and supporting substantial amounts of unused capacity.



> "It makes government a consumer of computing power, enabling the federal workforce to focus on fulfilling their agencies' missions and objectives."

Federal executives don't want to be data center managers, nor do they want the problems associated with legacy equipment hampering business operations and the delivery of services to citizens. For feds, cloud seemed like the perfect solution. Moving IT applications and systems to the cloud helps eliminate maintenance costs, giving agencies on-demand access to a pool of configurable computing resources that can be rapidly provisioned. It makes government a consumer of computing power, enabling the federal workforce to focus on fulfilling their agencies' missions and objectives.

Even so, change is difficult. While the cloud offers many advantages, there are also pitfalls. Storing data outside the traditional walled-enclosure of a federal building requires a change in thinking. And replicating and deploying assets from a physical space to a virtual one can also be time consuming and challenging. Finally, and perhaps most important for government, most cloud providers are not responsible, or at least not completely responsible, for the security of the clouds they host, so agencies still need to provide good security, and perhaps more so since data is not in their direct possession.

Those concerns hampered cloud federal cloud deployments, but even so, the Government Accountability Office estimated in 2015 that the government saved half a billion dollars with its limited cloud technology use over a period of about four years.

SOARING SAFELY IN THE CLOUDS WITH IMPRES

In the first chapter, we explained the IMPRES approach to networking, and how to achieve total security by removing the reliance on IP technology and numbers, replacing them with Identity Defined Networking (IDN) that has the power to cloak devices and make them unreachable for unauthorized users. The good news for cloud deployments is that the IMPRES approach was created with cloud in mind, and works just as well to protect networks there as it does for physical networks. And like with physical networks, IDN is completely platform agnostic. It works whether you or your host are using any mix of bare metal servers, storage, or networking devices, and also with VMware, KVM, OpenStack, HyperV, Azure, or Amazon Web Services.

Even the Conductor appliance, which is used to control IDN and enables software provisioning and other network manipulations, can run as a virtual appliance or even as a service from within any government cloud.

Beyond just IDN, the IMPRES approach helps to simply cloud deployments by relying on proven tactics and techniques to ensure that

everything can be spun up quickly, and maintained without any delays. For example, IMPRES engineers are experts in software-defined networking SDN), allowing for the rapid expansion of cloud services and resources on the fly in a matter of seconds. Your government cloud is always completely optimized for both performance and costs. Most clients find that their time to implement secure cloud-based networking is reduced by as much as 97 percent compared to working with any other method. And, every part of the approach is deployed by NetOps and easily verified by InfoSec.

Once deployed, IDN combined with SDN means that every endpoint, service, virtual machine and device within the cloud has their IP removed and replaced with a unique network identifier. They are undiscoverable from the outside or even internally to attackers trying to use standard IP-based tools. This reduces any cloud's attack service by as much as 90 percent, eliminating a key worry about federal cloud deployments.

The IMPRES approach also automatically puts fully-encrypted bridges between every single connection and device throughout the cloud. Unencrypted traffic or users trying to use IP services are immediately identified as likely attackers, improving the time to mitigation, revocation, and quarantine by as much as 25 percent compared to any other system. And, with powerful SDN tools and virtual networking, it decreases both failover and disaster recovery times to as little as one second. Should a resource go down or become compromised by an attacker, it can immediately be disconnected and redeployed, and the proper protection put in place to prevent future problems. All of this can be done automatically, or with human oversight.

By standardizing on the IMPRES approach, federal agencies can reap all the positive benefits of cloud deployments while mitigating the risks. A cloud network following the IMPRES approach will be completely cloaked from outside attackers and unauthorized users, and can be fixed and brought back up to speed in as little as one second with no downtime. It's everything that federal agencies need to go from dipping their toes into the cloud to diving fully in, safe in the knowledge that their cloud is far more secure and much less costly than any physical or virtual network they could otherwise deploy.

CHAPTER 3

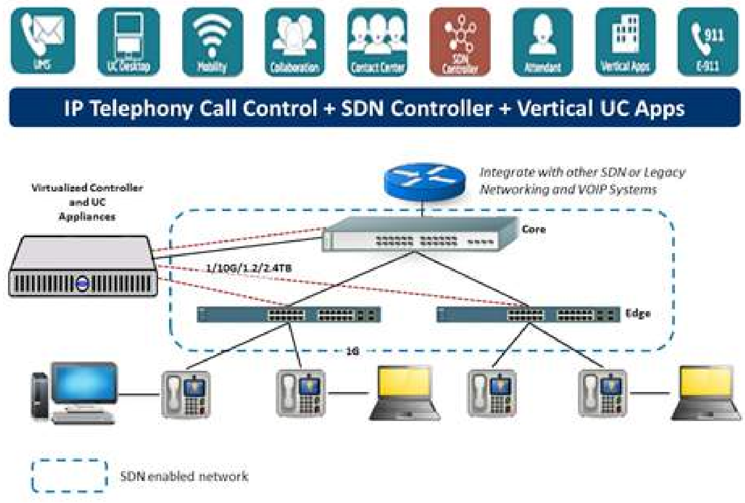
The IMPRES Approach to Proactive Threat Mitigation

THE WEAKNESSES OF A PURELY REACTIVE DEFENSE

Currently, even the best defenses within the federal government are passive and reactive in nature. Security solutions monitor network traffic looking for indicators of compromise, and send alerts back to SIEM defenses if something is detected. This triggers IT teams to react to try to mitigate the threat based on the information collected by the security appliance or software. In a perfect world where only one or two threats assault security perimeters each day, this is a perfectly acceptable system for providing a moderately secure network. But the time when these types of reactive defenses could ensure anything close to complete protection is long since passed.

The problem is that threats of all kinds are increasing exponentially, including the most dangerous, targeted ones that aim specifically at government agencies. In an era when over 200,000 new malware variants are created every single day, attackers can use the chaos of those incidental threats as camouflage to launch their targeted attacks, flying under the radar of many defensive systems.

The adversaries are very good at what they do, sometimes even trained and financially supported by nation states. Like any terrorist, they take their time to study their opponents,


UMS
UC Desktop
Mobility
Collaboration
Contact Center
SDN Controller
Attendant
Vertical Apps
911
E-911
IP Telephony Call Control + SDN Controller + Vertical UC Apps
Virtualized Controller and UC Appliances
Integrate with other SDN or Legacy Networking and VOIP Systems
Core
1/10G/1.2/2.4TB
Edge
1G
SDN enabled network

crafting phishing and other social engineering type attacks that have a high chance of success when deployed against distracted or untrained users who are tricked into giving them access to their local machine, which is then used to attack the larger network.

Once inside a network, they search for valid paths to travel alongside authorized users and processes, which allows them to jump to other systems. They move very slowly to avoid detection and try to blend in with normal network traffic. Even if their actions do eventually get flagged by security programs, there is a good chance that they have already been inside the network for an extended period of time. In fact, according to the Cisco 2016 Annual Security Report, the average time it took to detect attackers working inside a compromised network was between 100 and 200 days. And this was true despite a huge increase in cybersecurity spending across all sectors.

> "Attackers unfortunately don't follow a set schedule"

It's clear that reacting to triggers, generating alerts and then asking security teams to respond in a timely way is no longer a very effective way to protect a network, and certainly not good enough for our nation's most important cyber assets.

GETTING PROACTIVE ABOUT SECURITY POSTURES

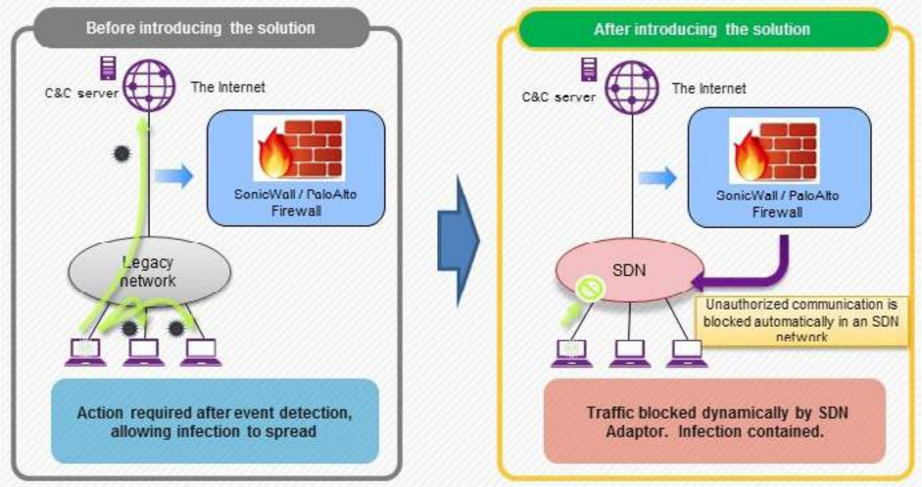
The best way to jump out of the way of a speeding train is simply to know the schedule and not be anywhere near the tracks when it speeds past. That is the basic idea behind the IMPRES approach to improving cybersecurity. Attackers unfortunately don't follow a set schedule, but they are surprisingly chatty about their intentions, and do a lot of collaborating with other attackers in their communities to share tips and tricks before major operations. You just need to know where to look.

The IMPRES solution enables government security teams to search tweets, the Dark Web, social media, chat lounges and even the temporary websites put up by hackers to communicate. It can translate multiple languages and search different media such as videos or podcasts. The threat intelligence it gathers can then be compared to actual assets, locations and government targets that attackers are planning to attack.

Back in chapter two, we learned that IMPRES engineers are experts in software-defined networking (SDN), allowing for the rapid expansion of services and resources on the fly in a matter of seconds. For cybersecurity, they can tap those skills to enable a more proactive approach to defending a network.

Let's say that the threat intelligence reveals that attackers are planning on using a certain family of exploits to get at data contained in a hardware-based server at a specific agency. Often, the collected intelligence is that specific.

In that case, of course the network can be hardened against that type of attack, but what about moving the target? Perhaps the data that is being targeted and the application that interfaces with it could be moved, temporarily or permanently, into the cloud? The IMPRES approach allows this to happen very quickly, with no change in network performance levels. That way, even if the attack somehow still gets through, the data that is being is no longer in place. It was moved off the tracks days or weeks before the train could arrive.


Before introducing the solution
C&C server
The Internet
SonicWall / PaloAlto Firewall
Legacy network
Action required after event detection, allowing infection to spread
After introducing the solution
C&C server
The Internet
SonicWall / PaloAlto Firewall
SDN
Unauthorized communication is blocked automatically in an SDN network
Traffic blocked dynamically by SDN Adaptor. Infection contained.

Should an attack still take place, threat indicators can be compared to the threat intelligence. If an attacker was planning on using a certain IP range, and the threat somehow connects to that, the data going to the SIEM can be elevated to the highest level because it contains evidence of being connected to a known and active threat.

Even if an endpoint is compromised, it can be immediately dropped from the network and placed into a quarantined area. It will only be allowed back into the network once it meets certain criteria, namely that the threat has been elimi-nated from it. Using SDN backed by solid threat intelligence means that this entire process can take place in less than a second. SIEM teams are still alerted, but are put in the role of confirming that the threat is gone, not rushing out haphazardly while trying to combat a dangerous, ongoing attack.

The modern threat landscape requires a modern solution. Only the IMPRES approach can marry deep threat intelligence with cybersecurity defenses, creating a moving and highly protected target that can stymie even the most advanced attackers.

CHAPTER 4

Empowering Federal Agencies Though Protected Collaboration

COLLABORATION FOR THE WIN

People work best when they can collaborate with one another. Collaboration allows multiple skill sets to be brought to bear against any problem. It can range from having an expert check someone's work, to having everyone put their heads together to address a particularly demanding situation, to accessing outside experts to obtain the opinions of the best and brightest minds in a field. Without collaboration, people must reinvent the wheel every time a new problem arises, even if others may have already done a lot of work on it, or even come up with a solution.

Yet, as powerful as collaboration is, it's always been an area where government struggles, especially compared to private industry, where the practice is much more accepted, if not embraced. But for government, the problem is that collaboration efforts often stumble over security regulations, best-practices and even mindsets.

Government has good reason to be wary of sharing its data through collaboration. The importance of the information created and protected by government is such that if it gets into the wrong hands, many people might suffer. Lives could even be lost. As such, government relies on various technologies like encryption to keep their data safe, but doesn't have an effective way to share that information or use it for collaboration, espe-cially with outside partners, without completely losing control over it.

DATA AT REST, SAFE AND SECURE

When working with data at rest, the government relies on encryption to prevent unauthorized eyes from prying, even going so far as to pioneer many of the standards and techniques that are the cornerstone of the technology. As far back as 1977, when the government standardized on the Data

Encryption Standard (DES), the technology has been used to protect vital information, even if it made collaboration efforts more difficult.

Over the years, various threats have developed to impede encryption, which only helped to push the advancement of the technology even further. In 1999, the Electronic Frontier Foundation along with distributed.net worked together to publicly break the encryption on a DES-protected document in just 22 hours. Suddenly, government found itself relying on a protection scheme that could no longer keep its secrets hidden.

> "Suddenly, government found itself relying on a protection scheme that could no longer keep its secrets hidden."

Reacting to that shocking development, in 2001 the National Institute of Standards and Technology (NIST) set a new standard of encryption for government use to replace DES. Called the Advanced Encryption Standard (AES), it uses three different key lengths, either 128, 192 or 256 bits. The 256 bit AES encryption is the most secure, though all three are considered almost completely unbreakable given today's technology.

Most information in government today is protected by locking down the drive or drives it resides on with 256 AES encryption. It's safe, but only at rest, which makes collaboration difficult. Some users even go so far as to remove files from their encrypted nests so they can be shared. Discouraged and sometimes illegal, the reason it happens is a byproduct of a two-choice system where you can either have safe data with no collaboration, or vulnerable information that can be shared, but that completely escapes an agency's control.

This goes further in explaining the need to use a technology like IMPRES Identity Defined Networking in conjunction with SDN network components to quickly revoke or grant access to devices, users, segments and even finite data sets across multiple planes of your network.

DATA THAT NEEDS TO MOVE

The IMPRES approach to collaboration uses encryption to protect data, but does it for data at rest and on the move. It allows data to be shared, even outside of an agency, without forcing government to ever give up control.

This seemingly magic trick to foster safe collaboration makes use of file-based encryption technology, as opposed to the more sledgehammer-like drive encryption, and a management program where an agency maintains all the encryption keys.

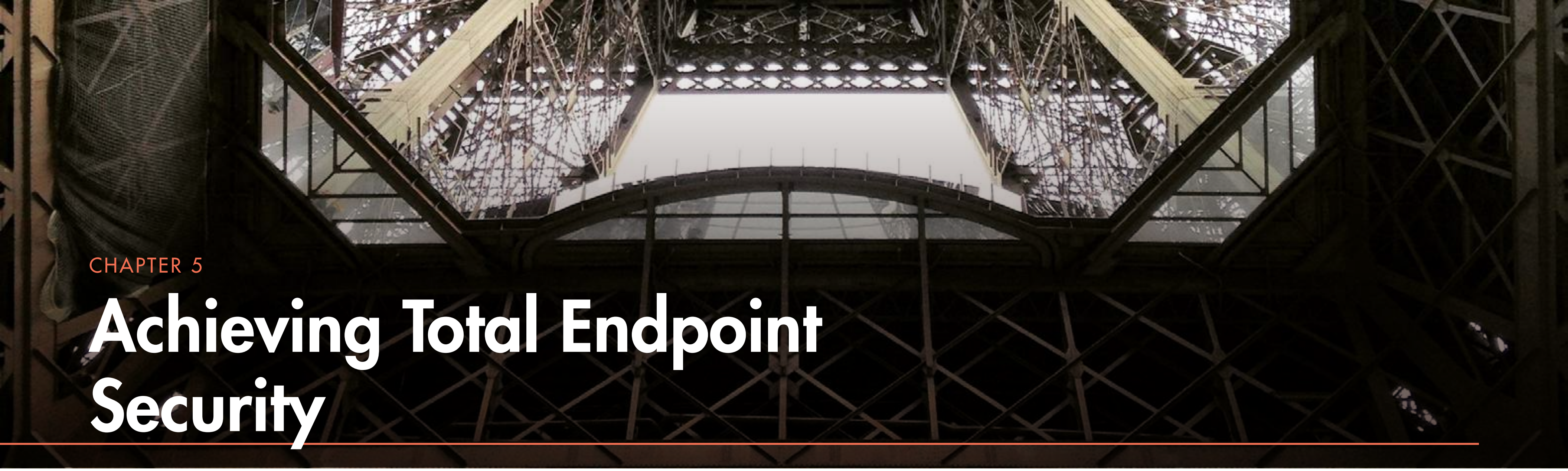
It works because each time an authorized user accesses a file, it checks to ensure that the user is authorized to view it. It doesn't matter where the file ultimately resides, on an agency server, in the cloud or on an endpoint. The file will only be unencrypted for valid users. Authorized personnel can access the file and collaborate freely as if the encryption protection didn't even exist.

The IMPRES approach allows this tech-

nique to extend outside of an agency's walls as well, without ever losing control of the data. For example, when a protected file is sent out via email, the user who is sending the email can enter the information about the outside entity who is authorized to view it. That same check is made on the other end, just as if the file was being opened locally. In fact, if the user does not have permission to make a file sharable, they can still send it out, but administrators will have to authorize the use of that key before the recipient can view it.

All keys are stored in a central management console and can be set to expire after so many uses, based on time or any other factor. Keys can also be rescinded at will, which makes the data unreadable no matter where it currently resides. You can even burn encrypted files to a non-writable media like a CD or DVD for sharing, and then expire the keys later to make them unusable, even if the CD or DVDs are hundreds of miles away, or their locations are unknown.

The IMPRES approach leverages the unbreakable encryption technology created and supported by government and adds the ability to allow for safe sharing and collaboration work. Data is always protected and access to it is always controlled, even when used for collaboration. It's the best of both worlds, and only available when standardizing on the IMPRES approach.



CHAPTER 5

Achieving Total Endpoint Security

ENDPOINTS AS GATEWAYS TO THE NETWORK

The federal government has a lot of users, and a lot of devices. In fact, it's one of the largest organizations in the world using computers. And those computers are no longer defined as just desktops or workstations. Many government agencies, especially those with large public outreach responsibilities, have found that relying on the mobility found with tablets, laptops and smartphones can extend the reach of government to more citizens, more quickly. Even agencies whose responsibilities are more internalized have found that untethering their workers from desks can reap huge productivity rewards.

But all that mobility comes at a price, namely an increased attack surface that hackers can exploit. Most advanced persistent threats (APTs), the tool of the modern attacker, are designed to first compromise a low-level endpoint within an organization before moving laterally deeper into the network, elevating privileges and creating a command and control capability which either slowly steals targeted data or opens holes for more advanced malware to follow.

With endpoints being the most popular gateway for launching attacks against federal networks, adding more operating systems like iOS or Android, whose protection schemes may not be as mature, only adds fuel to an already volatile situation. Hackers don't really care what kind of endpoint they compromise to start their advanced attacks. As a jumping off point into the main network, compromising a mobile device is just as good as capturing a traditional desktop.

ALL DEVICES GREAT AND SMALL

The good news is that the Identity Defined Networking (IDN) technology used in the IMPRES approach that was detailed in chapter one can also shield mobile devices from discovery or exploit. Each authorized mobile device receives a unique host identifier in the form of a long-lived CryptoID, and no longer uses IP technology to communicate when working in a federal network. Just like with desktop systems, mobile devices on the internal network will only respond to traffic from explicitly whitelisted systems or endpoints coming in through encrypted channels.

In fact, using IDN from the start with the IMPRES approach can ensure that endpoints are never put into a vulnerable state, even when being first added to a network. With IDN, endpoints are whitelisted, stripped of their IP dependency, and given a secure security identifier right from the start. They never have the same vulnerabilities as endpoints being deployed in traditional ways. Once installed, the IMPRES approach also protects agency assets with a 256 AES encryption lattice for all communications. Working in concert with SDN and IDN, allows endpoints to be quickly provisioned, deprovisioned, isolated, and interrogated or examined at will.

> "They never have the same vulnerabilities as endpoints being deployed in traditional ways."

The IMPRES approach can take BYOD programs into account even if an agency does not have complete control or ownership of the device, setting up a partition whereby the IT staff only manages and sees information and programs from the government part of a smartphone. Users working from the public part of the phone likewise do not have access to any government resources.

Even with IDN protections in place, its best to ensure that every mobile device is kept up to date with the latest patches and information. According to Verizon's 2016 Data Breach Investigations Report, most attacks still exploit known vulnerabilities that have never been fixed despite patches being available for months, or even years. In fact, the top 10 known vulnerabilities accounted for 85 percent of all successful exploits over the past year. Because of this, the IMPRES approach adds a full mobility device management (MDM) program for all tablets and smartphones.

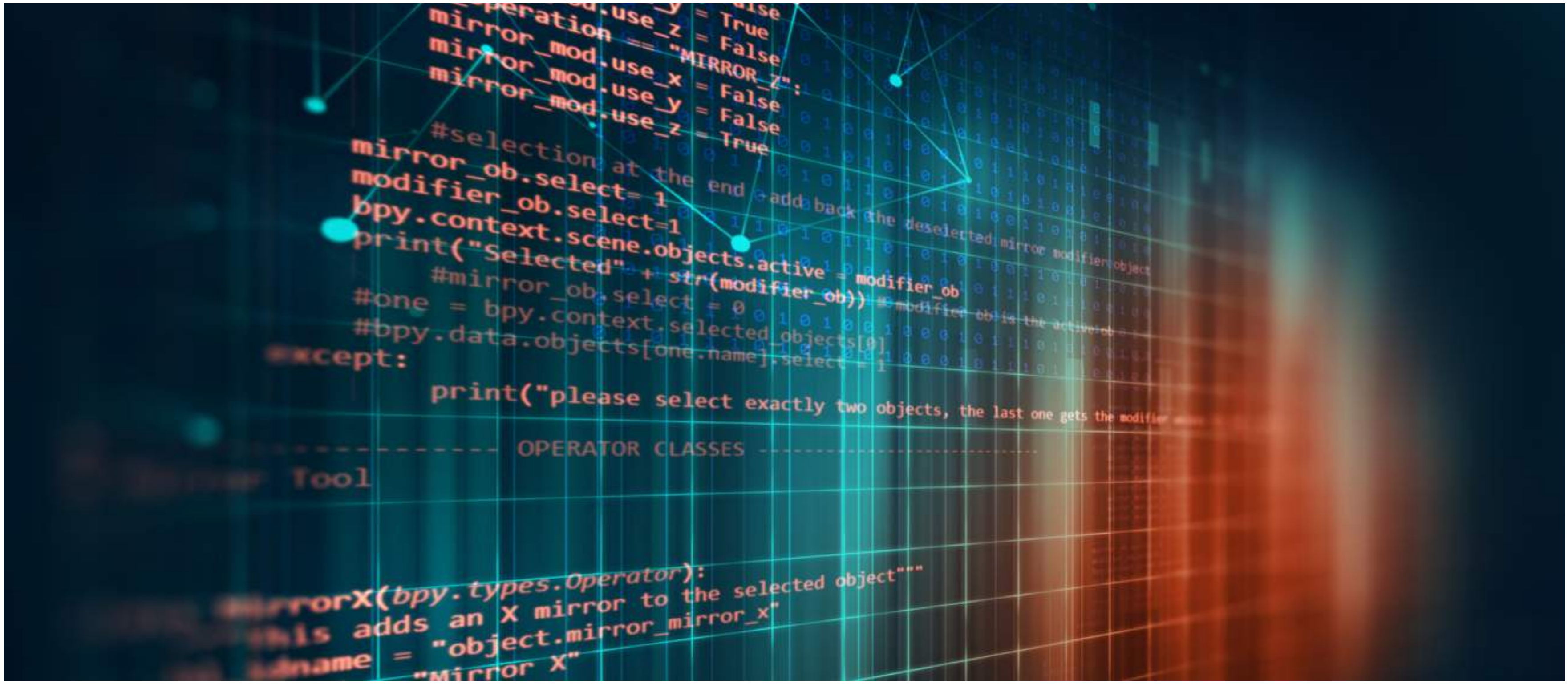
The MDM not only keeps mobile devices up to date with the latest security patches, but can also force them to comply with security policies before joining the network. Any device that is found not to comply with guidelines or regulations, like NIST's guide to Dramatically Reducing Software Vulnerabilities, the National Industrial Security Program Operating Manual or any number of other government or industry best practice guidelines, can be automatically flagged or even reconfigured to ensure compliance.

APPLYING ADVANCED ALGORITHMS

Having good, constantly updated security on mobile endpoints combined with protecting the backend network using IDN creates quite a digital fortress. But the IMPRES approach goes a step beyond that, installing some of the most advanced protection available on every single mobile endpoint to stop threats from ever deploying, even if a user accidentally, or is tricked through social engineering, from running them.

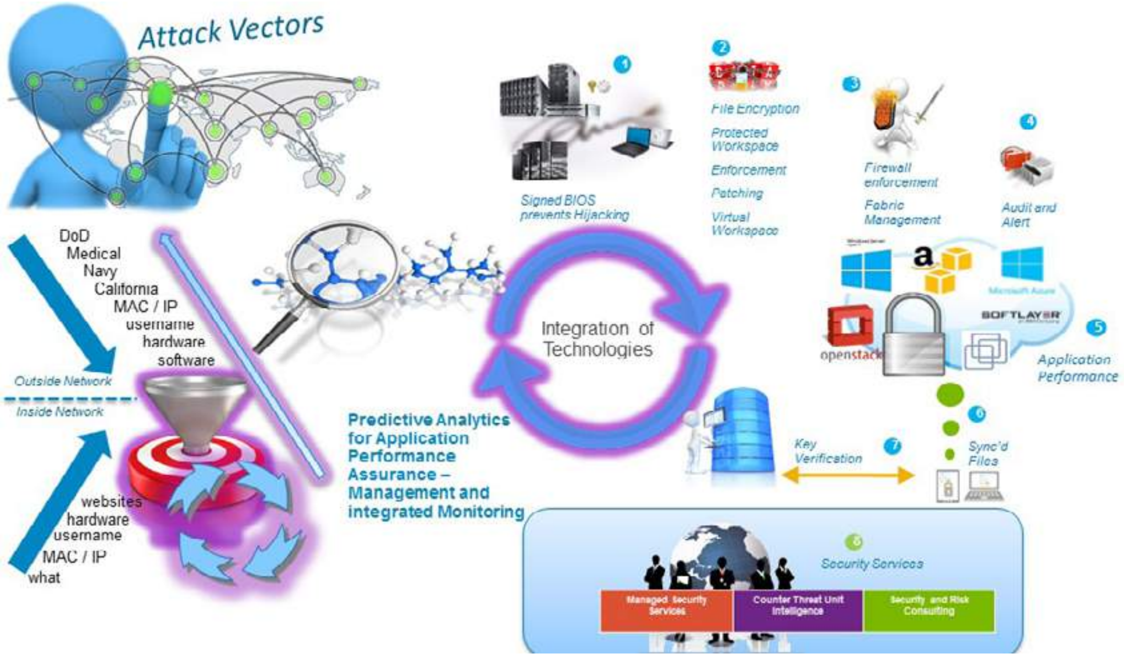
This extra step of protection is installed as a tiny program and works with any mobile device including laptops, tablets or smartphones, and most operating systems including Windows, Android and Apple iOS. It can be deployed as part of any type of mobility program including DoD or agency-owned, personally-enabled (COPE), choose your own device (CYOD) or bring your own device (BYOD).

Once deployed, it enables each mobile device to act as an advanced network sandbox. Applications that users attempt to trigger on the mobile device are first sent to the local sandbox and exploded. While there, advanced algorithms examine every aspect of the code, including what it is attempting to do and who it is trying to communicate with. It can determine the presence of malware or hidden exploits without having to rely on signatures. On most devices, it can accomplish this task in less than a few milliseconds, so users are never slowed by having the protection in place. If malware is detected, the program is


mirror_mod.use_x = False
mirror_mod.use_y = False
mirror_mod.use_z = True
#selection at the end -add back the deselected mirror modifier object
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
#mirror_ob.select = 0
#one = bpy.context.selected_objects[0]
#bpy.data.objects[one.name].select = 1
except:
print("please select exactly two objects, the last one gets the modifier
OPERATOR CLASSES
Tool
X(bpy.types.Operator):
adds an X mirror to the selected object"""
= "object.mirror_mirror_x"
"Mirror X"

blocked from running and the user is notified. A separate note detailing the incident is sent to the IT department for record-keeping or remediation. But the malware doesn't gain a foothold. Both the individual device and the connected network are protected.

Mobility can be a huge force multiplier for government agencies whether they are involved in providing citizen services, protecting the nation, or follow any other set of mission goals. Deploying the IMPRES approach can safeguard those mobile endpoints, providing all the benefits of a mobility program while eliminating the associated risks.



IMPRES
Technology Solutions, Inc.

DELL EMC
FEDERAL PARTNER
GSA AUTHORIZED