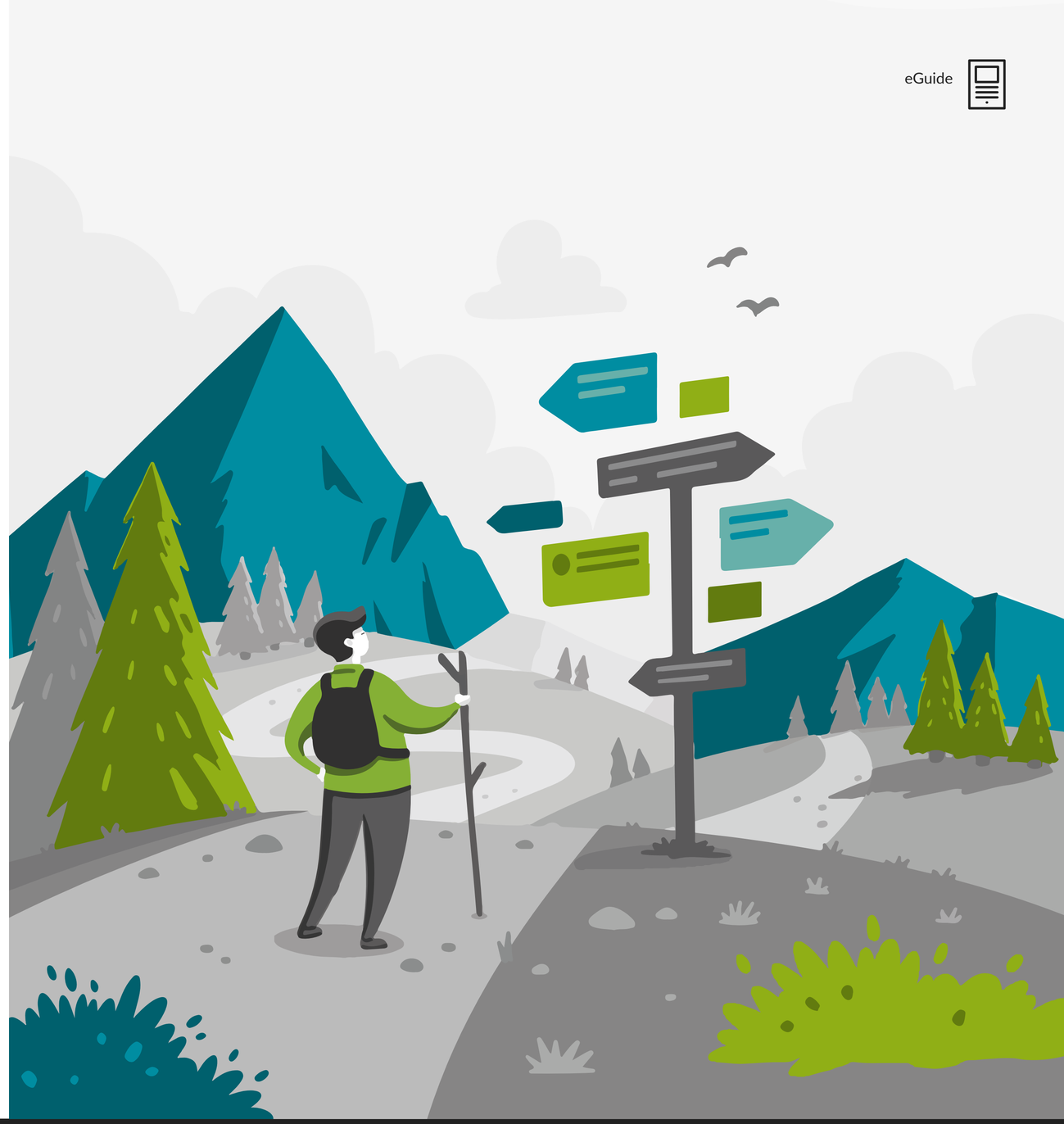
JUNIPER NETWORKS | Engineering Simplicity

eGuide

Understand the Basics of Cybersecurity.

By Trevor Pott
Technical Security Lead, Juniper Networks



Introduction

This document covers the fundamentals of information security, what it does, and why it is so important.

Information security or ‘infosec’, describes everything relating to protecting information: principles, tools, techniques, technologies, products, services, and practices. Infosec begins and ends with people – compromises happen almost exclusively because of a human failing of some kind.

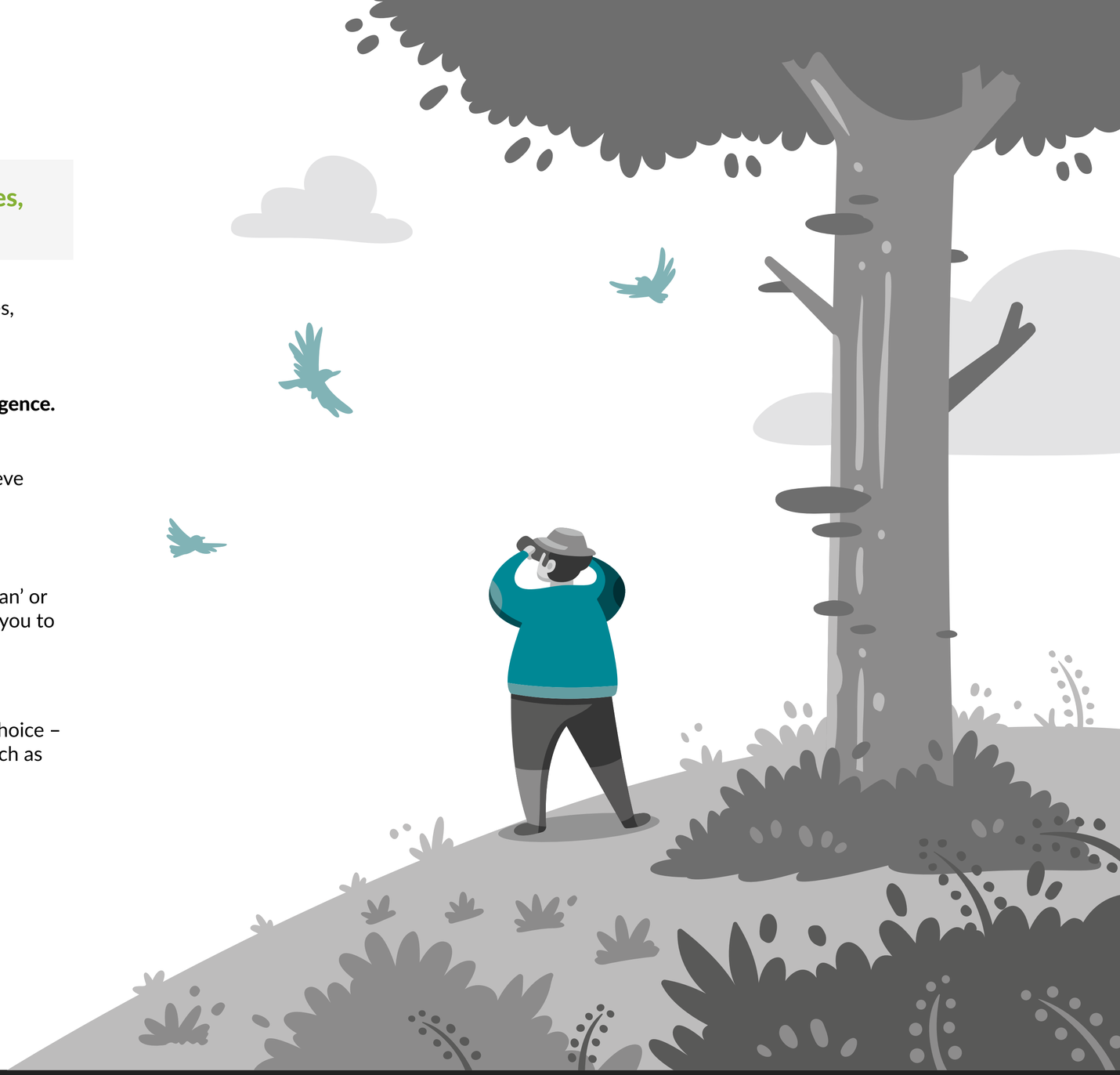
There are three main categories of human compromises: **ignorance, social engineering, and negligence.**

Ignorance is a lack of knowledge, and can be a security risk when we mistakenly believe that we know something that we do not.

Social engineering can be as simple as a fake call from a so-called ‘Microsoft technician’ or as sophisticated as a spear-phishing email leading to a replica website. It aims to get you to reveal details that give access to your accounts.

While all of us can be ignorant and vulnerable to social engineering, negligence is a choice – it requires someone to deliberately choose to put aside some aspect of their duty, such as educating themselves or performing a task.

Fortunately, technology can be used to help prevent infosec compromises by blocking attacks, sending reminders to operators, and detecting malicious, abnormal, or negligent behavior.



Basic IT Infosec

Data and Metadata

Most information is stored as data in a computer somewhere – not just as files or databases, but also as pictures, word documents, records, and so on.

Information about information, otherwise known as metadata, is also important.

Pictures often have metadata associated with them, such as GPS coordinates or details of the device that took the image. If this metadata is not stripped out when an image is posted to social media, then a malicious actor can use it to determine a target's location, and even what type of phone to look for to help identify that individual.

Consider someone taking a food selfie, and attaching it to a social media message. This gives the thief a location and a time; simple maths will tell them whether or not that individual can get back home before the thief can steal from them.

Metadata can also reveal corporate secrets. An electrician posting a picture about the cabling job they just completed on the new as-yet-unannounced data center, could easily give away its location to anyone looking at the metadata. Similarly, a Word document tends to keep a history of everyone who has edited it, which can have legal consequences.

Much More than Firewalls and Anti-Malware

Classic firewalls and anti-malware are not particularly effective on their own.

A classic firewall can prevent someone from remote controlling your PC, but it cannot filter out phishing emails that contain a link which, if clicked, will either download a remote control application that will work behind a firewall, or can reconfigure your firewall to allow remote access to your PC.

Similarly, anti-malware applications are quite good at defending against malicious files of a known type, but not so much against those it hasn't seen before – and they are virtually useless against the myriad of interesting things that can crawl onto your PC through an internet browser.

In enterprises, most infosec products and services focus their efforts on data in-flight – that is, data in transit – with the aim of catching whatever badness is happening before it reaches the user or leaves the network.

Next Generation Infosec

In the 90s, application-layer firewalls came into use, acting as a proxy between an application and the outside world. These were followed by Next Generation Firewalls (NGFW), which are more integrated into organizational infrastructure and bring advanced capabilities, such as applying policies based on user name or group, rather than just by IP.

In general, a NGFW prevents bad guys from getting into a network from the outside using basic attacks, they also offer some form of data-in-flight scanning capabilities, such as scanning emails for phishing attempts. NGFWs can protect thousands of users at once, and can defend endpoints incapable of using antivirus protection, such as printers.

Next-Generation Anti-Malware (NGAM) – or Next-Generation Anti-Virus (NGAV) – can only defend the host on which it is installed. So, it is used with NGFWs to help defend against social engineering attacks.

An NGFW tries to stop the badness from getting to your PC in the first place, which is the best, and safest, option.

NGAM (or NGAV) tries to prevent the badness from compromising your PC once it has got in – it's a last line of defense.

Basic IT Infosec

WAF and Application Security

The next evolutionary step is the Web Application Firewall (WAF). A WAF is an application-layer firewall that focuses on HTTP and HTTPS-delivered applications, typically ones that are accessed via the internet (within the network or externally).

WAFs protect against vulnerabilities specific to a given application, or class of application. For example, a WAF would filter out malicious SQL commands to prevent them from executing. WAFs are often used internally to protect against insider threats, and prevent one layer of an application being affected by the compromise of another.

Application security does not always rely on firewalls, anti-malware, or any other external product or service to provide security.

Traditional application security builds layers of protection directly into the application itself. Like anti-malware applications on a PC, application security is the absolute last line of defense for server-based applications. If an attack makes it that far, then something has gone horribly wrong with infosec along the way.

Defense in Depth

No single vendor can defend a network against today's threats, and no one has enough manpower or research and development capacity to chase innovative new approaches to counter emerging threats.

The only realistic way to defend a modern network is to have multiple products from multiple vendors working tightly together, providing multi-layered in-depth defenses.

Encryption and DLP

Encryption and Data Loss Prevention (DLP) are designed to prevent data inside the network from getting out.

Encryption technologies ensure that only individuals or applications with the correct key can access data.

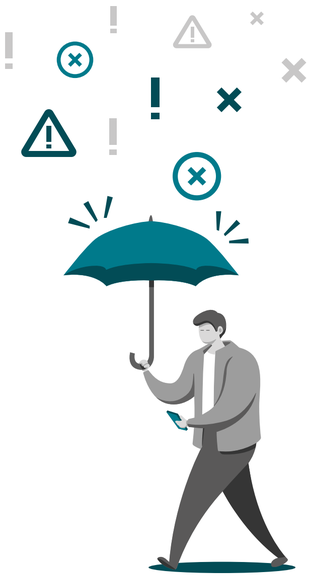
A lot of damage can be done to an organization if, for example, a sales manager's laptop is stolen, complete with unencrypted customer files.

Encryption on data in-flight is used to ensure that data is not snooped on by third parties – vital when accessing internet-delivered services, or anything over a wireless network (neither the internet nor wireless networks can ever be made 100% secure).

The basic DLP approach is to scan data attempting to leave the network, and stop it if it is not supposed to escape. It is often built into NGFW and NGAV, for example, to prevent files with certain types of content from being copied to a flash drive, or being uploaded to a cloud storage folder (such as Dropbox).

DLP is often incorporated into security tools that include Cloud Access Security Brokers (CASBs) and Advanced Threat Protection (ATP) products, which would, for example, detect transmission of a spreadsheet of credit card information and generate an alert or a block.

However, there are many more ways to sneak data out of a network: instant messengers, Slack, and social media are all poorly covered by modern DLP.



Basic IT Infosec Defenses

Monitoring

Without monitoring, IT practitioners would have no way of knowing what is happening, or what problems need to be responded to. Most monitoring products spot patterns using deviation and correlation.

Deviation relies on observing workloads and data flows between systems in real-time to establish a baseline of what 'normal' looks like, and then identifying departures from that norm.

Correlation-based monitoring looks for multiple events occurring at the same time, or in rapid succession, that indicate a problem, and is usually based on the event logs generated by applications or infrastructure components.

The ideal monitoring-based DLP system examines data access across the entire organization's IT infrastructure, looking for abnormalities. So if, for example, a sales manager who normally only accesses information on a handful of accounts a day suddenly pulls information on all accounts in their region, the system spots that something untoward might be happening. This approach requires multiple products from multiple vendors working together.

However, total monitoring of all of an organizations data is often impossible. Enterprises can have data in thousands of different locations and systems, both on-premises and in the public cloud.

Even if an organization could monitor all data access, there is the question of what to do about it: abnormal access patterns could be an employee trying to steal data, a compromise event occurring because of an external attacker, or simply someone trying to do their job. Increasingly, machine learning is being used to fine tune these patterns, and is likely to see significant development in the next few years.

SIEM and ATP

Security Information and Event Management (SIEM) products are the hub of infosec, and are increasingly interwoven with ATP products. They receive data from a number of products, and the most useful have quick and simple integration with leading products from multiple vendors.

The most successful SIEMs and ATPs are focused on correlation. Here's an example.

1. The NGFW sends email data streams to the ATP, which detects a series of malware-laden emails targeted at a given user.
2. The ATP instructs the firewall to prevent the emails from arriving.
3. Shortly afterwards, the NGAV on that user's endpoint detects strange behavior.
4. The CASB detects that the endpoint is attempting to connect to cloud storage sites and upload documents.

While the severity of alert for each event is likely to be low, if the ATP correlates them it can determine that a targeted attack is probably taking place, declare it a maximum threat, and call for a human.

SIEMs mainly collect event and monitoring data, and many vendors have started adding scanning capabilities, building in DLP, or enabling integration with an application that has DLP.

Basic IT Infosec Defenses

Access Control, VPN and Remote Access

Thanks to infosec technologies like encryption, it is possible to have physical access to a storage device but not have access to the actual data. Similarly, cloud computing can allow organizations to have access to products, services, and data from anywhere in the world without ever having access to the underlying hardware.

Virtually every piece of IT infrastructure, operating system, and application has some form of access control. Among the two most important methods of access control are Virtual Private Networks (VPNs) and remote access.

VPNs are encrypted network tunnels between two computer systems. They are used to allow individuals to connect securely to their organization's private network and to establish secure links between sites. They also use encryption to protect against snooping by malicious actors.

Remote access is the term used for any number of technologies that allow individuals to access organizational resources without using VPNs.

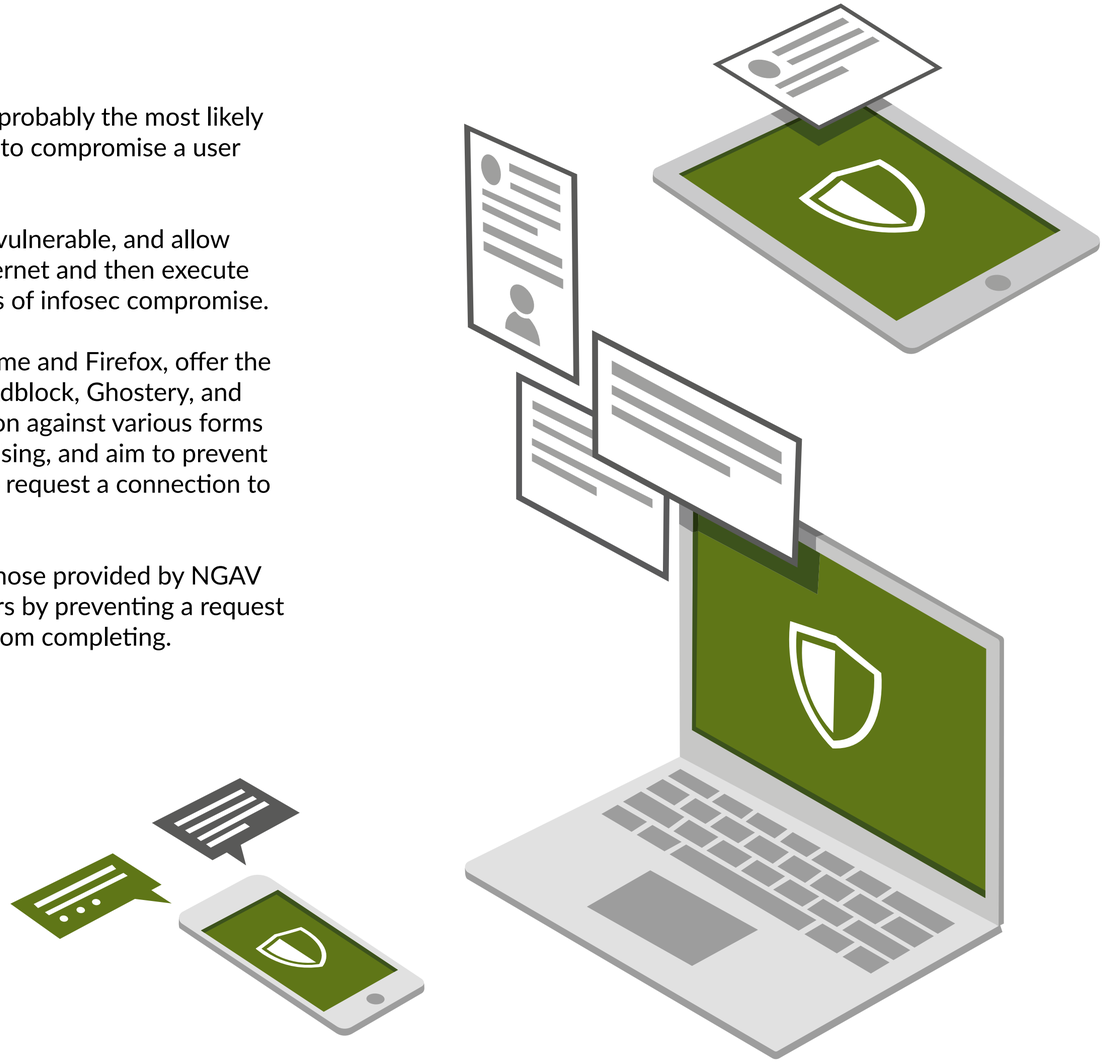
Browser Defenses

Aside from email, web browsers are probably the most likely route for an external attacker to use to compromise a user device or endpoint.

Today's web browsers are still quite vulnerable, and allow users to download files from the internet and then execute them, the third most common means of infosec compromise.

Popular web browsers, such as Chrome and Firefox, offer the ability to install extensions such as Adblock, Ghostery, and Privacy Badger, which offer protection against various forms of internet badness, such as malvertising, and aim to prevent the web browser from attempting to request a connection to suspicious internet resources.

Other browser extensions, such as those provided by NGAV vendors, attempt to protect end users by preventing a request to access a compromised resource from completing.



Basic IT Infosec Defenses

MDM

Mobile Device Management (MDM) products are designed for devices that live outside of the organization's perimeter, such as cell phones, tablets, and laptops. They apply security templates, profiles, and policies to remote and mobile devices, and ensure that they meet organizational infosec requirements before being able to connect to resources behind the corporate perimeter.

MDM provides secure application delivery via solutions, such as app stores and Virtual Desktop Infrastructure (VDI). MDM products also address access control, ensuring that only the authorized user can use the device, and enabling tracking or remote wiping if it is stolen or lost.

Authentication

Centralized authentication and Unified Authentication (UA) technologies rely on directory services such as LDAP, SAML, or Microsoft's Active Directory. Single Sign-On (SSO) is the most recognizable UA technology, and aims to allow users to use a single username and password to access workloads and services from multiple providers, located on multiple different infrastructures.

Multi-Factor Authentication (MFA) systems are also widely used, but can cause complications if, for example, they need to differ based on country. For example, SMS verification (a common MFA approach) requires users to enter a code from a text message to log in, yet many countries implement restrictions on SMS messages that can make this unreliable, or require additional integrations to work properly.

Automation

The number and diversity of workloads under management is growing fast. The rate of change in IT hasn't stopped accelerating for some time, and humans can't keep up without help. This is where automation comes in.

Automation is the most important infosec defense of all.

Due to the highly interconnected nature of today's IT, the rapidly vanishing network perimeter, and the fact that threats can and do happen from behind the perimeter, infosec must be a part of all aspects of IT. Every piece of IT infrastructure, every workload, and every network-connected device must be part of an organization's infosec design.

Anatomy of an Attack

Defining the Objective

Imagine a hacker; we'll call him Bob (there are female hackers, but statistically, the criminal ones are more likely to be male). Bob's target is PotatoCom, a local internet service provider. PotatoCom has refused to install fiber-optic internet for the umpteenth year in a row, and Bob is sick and tired of terrible ADSL. As an act of revenge, Bob wants to compromise PotatoCom's financial system by denying them access to their own database.

To gain control of the system to carry out his plan, Bob doesn't need to be some super-technologist, he only needs to learn enough to achieve his goals.

Connectivity

Bob needs to find a way to perform his illicit online activities in a way that cannot be traced to him. He could use unsecured public Wi-Fi in a coffee shop, but he'd have to do it without showing up on surveillance cameras, including those he will pass on the way there. To protect himself in case he passes a camera he cannot avoid (or failed to detect), he might use physical disguises.

He'll never use the same Wi-Fi hotspot twice, and varies the type of transportation he uses to get to various free Wi-Fi locations, to avoid creating a noticeable pattern of activity. If Bob can get close enough to connect, he might not even have to enter the building of the business providing the free Wi-Fi.

Bob also needs to hide his activities from any surveillance technologies on the networks that he is using. He will probably need to use a VPN, or more than one. He might also rent a VM or virtual private server as a place to stage his attacks. To further hide his internet traffic, he will probably use TOR, I2P, or another method of anonymization and encryption.

Paying

Every time he wants to go online, Bob needs to buy USB Flash drives, notebook computers, two VPN service accounts and two private VM rentals. So, he has to think through how to do that without being identified. There are ways of doing this – they may be convoluted, but it's possible. To cut a long story short, Bob (legally) manages to convert his cash into a pre-paid credit card that he can use anywhere, and which cannot be traced back to him.

Research

Bob needs to find out which database and backup systems PotatoCom uses, and how to get into their systems. He can use technical means to probe PotatoCom's IT infrastructure; he could use social engineering to chat up various PotatoCom employees, presenting himself as a knowledgeable individual (or an insider) and give people scope to vent, which usually works. He could also find what he needs on social media by looking for PotatoCom employees griping about the tools they use. Bob could even try calling up some of the vendor support lines and pretend to be from PotatoCom, just to confirm that PotatoCom is a customer.

Anatomy of an Attack

Getting into the System

The simplest way to get into a system is to socially engineer someone into giving their valid credentials for login. Bob doesn't need admin credentials – anyone who can see the infrastructure is just fine, even if they can't modify it. From there, he could use network scans to probe the infrastructure and use lateral movement to attack soft targets. Once there are multiple backdoors into the system, Bob could try technical stuff to get into the database and corrupt entries – but this is the hard way.

All Bob really needs to defeat PotatoCom's security is their administrative password.

They've got their entire infrastructure on a single cloud provider, so it's a good bet that they use the same administrative credentials for their production environment as they do for backups (not a security-savvy practice, but it happens).

Getting to Know the Target

Bob is unlikely to be able to socially engineer his way past someone with admin credentials, as they tend to be more security-conscious. So, he identifies a suitable target and uses physical surveillance.

Bob learns about his target and uses that knowledge to find the vulnerability that will let him obtain the admin credentials he wants – one way or another.

For example, homes are never secured as well as offices, and there are lots of opportunities to spy on people in their own home. If the target doesn't work from home, where is their office? Bob could socially engineer his way into the office and plant a camera or keylogger, spy through windows, or intercept signals from a wireless keyboard.

Thinking Like a Hacker

Once connected to PotatoCom's infrastructure, Bob disables change reporting features and corrupts the database. He then backs it up and deletes older backups, changes PotatoCom's password, and burns any evidence.

PotatoCom's financial database is now unusable, and they can't get access to their account to figure out what went wrong. They cannot bill their customers, pay suppliers, or file taxes. They may trigger an audit and get into trouble for not having access to the required data. They might even go out of business.

Nothing Bob did was technically difficult. What mattered was mindset. Bob went to great lengths to avoid identification. And he looked for the easiest way in – the most exploitable part of any system is usually the human being responsible for it. That's how a hacker thinks.

To defeat a hacker, a defender needs only the right mindset: safety first.

A defender needs to think like a hacker – looking for the exploits – and plug those gaps with technology, business processes, or even just curtains at the window. Defenders discover the tools they need to use once they know what they are defending. Just as with hackers, the mindset is what matters.

Advanced Concepts

Regulatory Compliance

Increasingly, it is not enough to simply implement infosec technologies, or pass an audit by applying IT policies in a tick box fashion. Organizations are being asked to demonstrate that they actually understand the basics, and why infosec is necessary.

The European Union's (EU's) General Data Protection Regulation (GDPR), for example, requires any organization involved in large-scale data handling to have a Data Protection Officer (DPO). DPOs are responsible for guaranteeing organizational compliance with the GDPR, and there are personal and significant financial ramifications if the DPO or organizations they work for are negligent in securing the data of EU citizens.

Segmentation and Microsegmentation

Network administrators use segmentation and microsegmentation to help prevent the lateral movement of any attacker who succeeds getting past a network's perimeter defenses. Each segment (or microsegment, which contains only one application) is separately defended. This kind of ring-fencing is protection against lateral attack, which is particularly important in shared environments, where IT infrastructures have multiple tenants, such as cloud service providers.

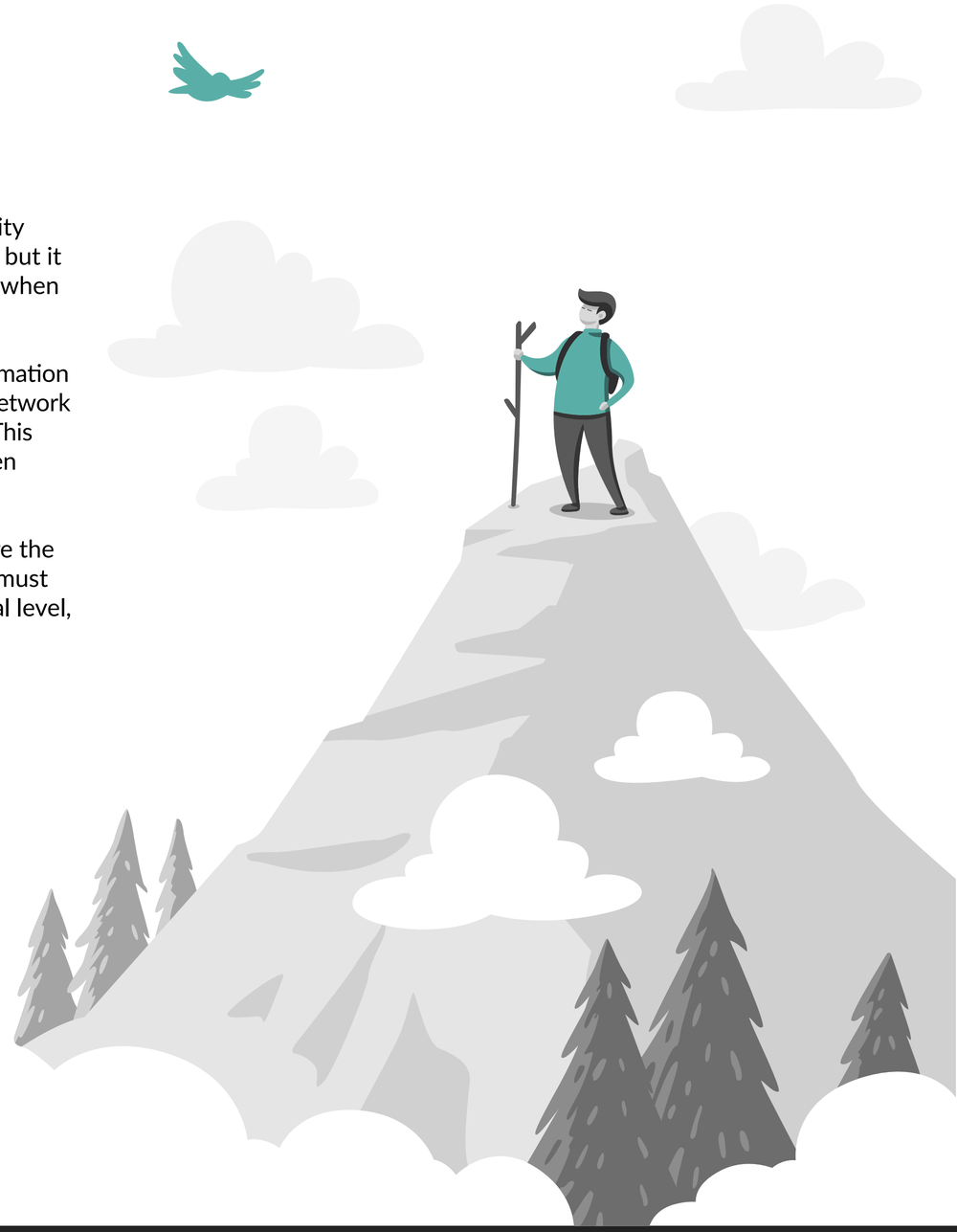
For example, microsegmentation would be an advantage in a research hospital. Rather than having each research project purchase its own IT infrastructure, using private clouds combined with microsegmentation, and appropriate infosec measures, can isolate each project as a tenant on the shared hospital IT infrastructure.

Putting It All Together

Infosec compromise events are a part of life. The inevitability of compromise doesn't invalidate prevention technologies, but it does mean that organizations must plan for what happens when a compromise occurs.

When tied into detection and mitigation technologies, automation can be used to trigger mitigation steps, such as ordering a network switch to disconnect or quarantine a compromised device. This prevents lateral spread, and can save enterprises tens or even hundreds of millions of dollars per event.

Prevention, detection, mitigation, and incident response are the four areas of infosec responsibility to which organizations must attend – always remembering that at the most fundamental level, information security is all about mindset.



Juniper Connected Security

Security Needs Layers

Defending today's networks means defending everything on those networks, and that requires a different approach to infosec than practiced by most organizations.

Networking and security are interconnected, and when people attempt to architect their networks using point solutions, things tend to go horribly wrong. Effective network security comes from interconnecting multiple layers of security, achieved by deploying multiple technologies, from multiple vendors.

Switches, routers, and Wi-Fi access points participate in Juniper Connected Security, providing deep network visibility and points of network policy enforcement, all centrally automated and orchestrated. This gives organizations the lateral protection that otherwise can be difficult to achieve.

While analysts might suggest that the best solution for a given segment is likely to be one provided by a specialist point player, this approach would require organizations to use multiple products and then get all the various bits to play nice with one another. This can make automation and orchestration of network defenses difficult: rankings change all the time, and automation implementations often outlast the lifecycles of the products they are automating.

Many vendors have a diverse portfolio of networking and infosec products, including partner ecosystems. There are also many others – like Juniper – that support customers operating at service provider scale, and can handle the craziest, most outsized networks that any enterprise customer can dream up.

What sets Juniper apart is the 'connected' in **Juniper Connected Security:** our commitment to interconnectivity. Juniper champions integration and orchestration, encouraging the use of open standards, open protocols and open APIs, and even builds in support for competing products. Our goal is to help customers make the best use of what they already have, instead of demanding that they rip and replace.

The use of a single operating system, Junos, throughout Juniper's portfolio makes centralized management much simpler, and enables Juniper to offer feature rich management platforms with management plans that are on-premises, cloud-based, or a combination of both. Junos OS makes adding functionality throughout the portfolio economical.

Juniper Connected Security gives organizations the ability to safeguard users, applications, and infrastructure, by extending security to all points of connection across the network. Enforcing policy as close to a threat as possible reduces the risk of that threat spreading. And through the use of machine learning, advanced analytics, and automation, rapid incident response becomes a reality.

Learn more about Juniper Connected Security in action.

Read now

Read the complete Basics of Cybersecurity Book here

JUNIPER NETWORKS | Engineering Simplicity

PN: 7400127-001-EN

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701