We have created a global society of universal connectivity, where individuals and organizations expect to have instant access to data and services across a variety of interconnected devices. It’s transforming our society. And it’s creating a rich vein of valuable information, goods and computing resources for our adversaries to extract, extort and exploit.
**Artificial Intelligence: Friend And Foe**

Artificial intelligence has a huge role to play on both sides of the cybersecurity equation. The industry faces a protracted and severe skill shortage. AI can perform both rote management tasks more quickly and efficiently, without getting bored or distracted. It can also learn new and better security practices from the evolving digital framework it inhabits. In our world where connectivity has far outpaced security, intelligent agents that can heal and defend themselves are invaluable allies. Machine learning has already proven effective in sandbox environments at exploring potential vulnerabilities and devising defenses.

But cybercriminals are developing their own AI, and are unlikely to do so ethically. In legitimate lab settings, AI can be carefully monitored and trained for years to be predictable and reliable. Cybercriminals are less likely to avoid these potentially dangerous side effects, favoring speed over safety. Malware rings resembling intelligent swarms of angry bees are already starting to appear, weaponizing IoT devices against their owners.

It is the rise of the hive. Today, the term botnet refers to automated, zombie-like devices that are remotely programmed to target other vulnerable systems with malware, or to infect them via blunt-force attacks, such as denial of service. Botnets are dangerous and account for billions of unauthorized network communications every quarter. The hivenet, however, is much more frightening because each unit of the hivenet, a swarmbot, will itself be powered by AI. Swarmbots will be able to make autonomous decisions without relying on a botnet herder and join together into larger autonomous thinking networks. The potential for hivenet damage is substantially greater than anything we have faced from already-potent botnets.

That’s why one of the most serious threats we face in 2018 and beyond is malware with the capability to learn and grow through its own successes. Polymorphic malware with pre-coded algorithms designed to subvert countermeasures and screens is already a reality. But that approach simply generates millions of slight variations on the same theme. Next-gen AI-generated malware will be aware and capable of adapting itself. Instead of simply following a set of pre-programmed instructions, it will select targets of opportunity, assess their weaknesses, develop a plan of attack and cover its tracks. And it will make intelligent decisions about what information to exfiltrate, and when. In short, tomorrow’s AI attacker will behave with the autonomy and inventiveness of a highly skilled and motivated human attacker, but at frighteningly higher speeds.

Hostile AI will be extremely dedicated to exploration, finding weaknesses at every possible crease in the network perimeter. Without any need for operator intervention, it will be able to fully map targets, design and deploy exploits, and even collect (and spend) ransoms.

These are not fever dreams. These are the clear and demonstrable goals of the cybercriminal branch of artificial intelligence research. Unsupervised, unfettered AI poses a massive threat to data security and infrastructure integrity.

We are at a very delicate moment in our transformation to a digital society and economy. Humans and machines must work together to prepare for the next level of sophistication.
Mobile Attacks Will Intensify
Mobile devices are small, powerful, always on and always connected. They have access to some of the deepest details of our personal and professional lives. They have sensors that can take detailed records of our every move. And that's why they are the target of more than 1 in every 10 global cybersecurity attacks. Designing and deploying remote jailbreaks that can completely subvert a mobile phone to an attacker's control is big business, and it's getting bigger.

Distributed Infrastructure Intensifies Risk
In a recent Fortinet Threat Landscape Report, the median organization responding to the survey used over 60 cloud solutions, roughly divided between software and infrastructure clouds. With this complexity comes increased risk. When organizations rely on dozens of different providers, they provide dozens of potential attack vectors. There were compelling business cases for embracing such a distributed and highly elastic infrastructure, but we are seeing the consequence today. It is extremely difficult to gain complete visibility into and control over every potential security weak point.

And distributing network resources has not distributed risk. In fact, we see the exact opposite: Global resources are more closely interconnected than ever. This phenomenon, called network hyperconvergence, means that we tend to see major attacks span multiple industries and regions all at once.

Encryption Is Confounding Early Warning Systems
There is a growing push for end-to-end encryption, particularly through HTTPS. We saw total HTTPS traffic eclipse in-the-clear HTTP in 2017 at 55 percent and climbing. All that encrypted traffic comes at a cost for threat monitoring and detection. Encrypted traffic is not inherently safe, it is merely obscured from prying eyes. And that can include the perimeter defenses meant to scan traffic and identify malicious activity.

Because it is more difficult for automated threat detection to scan encrypted traffic, attackers can actually slip past some screens by including malware in HTTPS sessions.

The end-to-end encryption trend is unlikely to reverse for other valid reasons, so organizations will need to continue to dedicate resources both to inspecting encrypted traffic when feasible and to finding ways to prop up other areas of protection where perimeter scans are less effective.

Ransomware Will Continue To Follow The Money And Expose Deep Vulnerabilities
The cost of disruption from high-profile ransomware attacks has significantly outstripped the amount victims have paid; for the most part, those hit by attacks like WannaCry have not paid their malefactors. The black hats carefully chose targets that deliver crucial services, like healthcare, financial services and critical infrastructure, hoping that the need to keep the lights on would force victims to capitulate.

Expect them to double down on this strategy and go after cloud services. Getting the upper hand on a major cloud infrastructure provider would represent tremendous leverage, potentially affecting service for millions and millions of users and undermining millions of dollars in daily revenue. It's happening already. Recently, a South Korean hosting provider paid a $1 million ransom to restore services.

Ongoing attacks against critical infrastructure providers will expose the fact that these networks are among the most vulnerable in the world.

—Derek Manky

A Clear Need For A Security Fabric
Considered individually and collectively, the scope and severity of the threat landscape underscores the need for a new approach to cybersecurity. We have no shortage of monitors, alarms, workarounds and procedures in our defense tool kits. What we need now is a more active and coordinated way to unify them at speed and scale as a cohesive security fabric.

An integrated, collaborative and highly adaptive security fabric will put AI and self-learning to work on effective and autonomous responses to attacks. It will combine technology, configuration, intelligence and judgment to perform basic security functions and day-to-day tasks currently being performed by workers. This will enable those individuals to focus on creating security principles and practices relevant to the highly organized opponents we face. And it will transition us away from organic and accidental network architectures toward a new design capable of standing up against intense, relentless, sustained attack.

Our adversaries are adopting automated and scripted techniques, so we need to raise their price of attacking to combat today's new normal. The time to watch and react is past. In 2018, cybersecurity must become proactive.