SMART PREVENTION
EXPECT THE UNEXPECTED
SMART PREVENTION – EXPECT THE UNEXPECTED

The political world is currently dominated by binary decisions, with voters asked to choose between diametrically opposed views. In the security industry, the choice between prevention and detection has often been presented in a similar way – almost as a philosophical choice of approach. When organisations first heard the ‘not if, but when’ mantra from technology vendors, some chose to place a disproportionate number of security eggs into the detection basket. But as attackers have become increasingly creative, reaching corporate resources with ever-more complex attacks, enterprises are drowning in detected issues – let alone those they do not know about. A recent study from the Ponemon Institute stated that over 90% of enterprises have vulnerability backlogs of up to 5,000. An over reliance on detection is not working.

So why did faith in prevention falter? Zero-day and advanced persistent threats emerged that could bypass traditional security controls such as AV, that relied on having seen a threat before. These controls could only catch what they expected to see. At the same time, evasive malware rendered many sandboxing solutions ineffective, as well fruitlessly and frustratingly slowing down business.

Check Point and BT have always maintained that effective cybersecurity should never be a binary choice between prevention and detection. Both capabilities form part of a well-designed, layered cybersecurity strategy. But we have also both argued the case for a proactive rather than passive approach. Now, through our continuous innovation, enterprises can implement and maintain proactive protection that eliminates even unknown and highly-camouflaged threats – before they reach users. With smart prevention, organisations can now confidently expect the unexpected.

“As the risk of digital crime grows, I believe businesses must be proactive”

Sir Michael Rake, Chairman, BT Group Plc
A PROACTIVE APPROACH GIVES ORGANISATIONS BACK THE UPPER HAND

Board members are now more aware of the increased threat of cyber-attack. In a BT and KPMG\(^1\) study of 2016, 73% of respondents said digital security was on the agenda of board meetings at least quarterly, if not more frequently. But in our experience many executives still fail to understand how every aspect of their business now relies on IT; and as a complex, interconnected digital ecosystem organisations are at risk from one cleverly crafted, highly-targeted email with a malicious attachment. Perhaps this is why so many attacks still take businesses by surprise.

When the German Federal Office for Information Security revealed that an unnamed German steel mill had experienced ‘massive damage’ following a cyber-attack, there was apparent disbelief. It was reported that hackers had infiltrated the company’s corporate network with a phishing email that tricked employees into opening a malicious attachment. Once the malware was installed, the attackers were able to move laterally within the steel mill’s IT systems – damaging the production network so that a blast furnace could not shut down, causing significant material damage\(^2\). At the time a digital expert said:

“We do not expect a steel plant to be connected to the internet and to be hackable – that is quite unexpected.”

Every business is a potential target and must take a proactive approach to counter the loss of data that has increased by 400% in the past three years. In the case of the unsuspecting German steel mill, we do not know if the malware embedded in the email attachment was known or unknown; but with our latest prevention solution this is immaterial, as Check Point and BT work together to help organisations expect the unexpected.

\(^1\) BT and KPMG – Taking the offensive
\(^2\) Guardian https://www.theguardian.com/public-leaders-network/2015/oct/14/how-to-stop-cyber-attacks-on-your-organisation
NEW PREVENTION CAPABILITY WITH CHECK POINT AND BT

In addition to getting the basics right to counter known threats, organisations need to enhance their prevention capabilities to manage the risks of threats they have not seen before. Attacking with unknown malware increases the likelihood of success for cybercriminals, who need fewer attempts to yield greater results. Even a slight modification to existing malware creates a new, unknown variant that could evade AV solutions. With nearly 12 million new malware variants being discovered every month, more new malware has been discovered in the past two years than in the previous 29 years combined. In the case of the German steel mill the impact, if not immediate, was obvious – but this is not always the case. Statistics show that in some cases, organisations take an average of 256 days to detect a breach, by which time it is far too late to take positive action and reduce the impact.

Managing the risk of new, unexpected malware will require organisations to do things differently, particularly as malware continues to target the files we trust and work with every day, such as PDF, Flash, or Microsoft Office. These files form the life blood of many businesses and hold much of their most sensitive data. But whatever solutions organisations choose to enhance prevention, they do not want to repeat the common frustrations with traditional sandboxing that introduce unacceptable delays to file delivery, or let potential threats through while evaluating files.

One of the priorities for any prevention solution must be fast, secure delivery of content that businesses can trust. Check Point and BT are delivering this by combining the most granular CPU-level exploit detection with expert human analysis. In this way, we can expose and help action the most unexpected and camouflaged threats before they enter your network – without slowing down or disrupting users.
BECOME A MOVING TARGET WITH CHECK POINT AND BT

Preventing attacks before they damage an organisation and creating a unified security architecture to simplify and harden security is a must in today’s threat landscape. As we have discussed, a mature security strategy will integrate smart prevention with detection and response to maximise every penny of security investment.

Analysts now advise that organisations seek technology solutions that not only integrate but also fulfil multiple criteria to reduce complexity. One additional benefit of the latest prevention solutions is that they can also be used to rapidly uncover existing vulnerabilities and – in the case of Check Point’s SandBlast solution – deployed to accelerate incident response. Organisations can use the actionable forensics data that the solution collects on user systems, to establish a detailed understanding of the attack flow, malware entry points and the scope of the incident. Add human enrichment to this from BT’s expert analysts and you can achieve a contextual, prioritised view to give you practical next steps.

Check Point and BT are working with organisations to develop a multi-layered approach to security – making it harder for criminals to operate before, during and after an attack. With Check Point and BT providing a partnership of technology and skills to disrupt attacks before they happen and proactively protect your most important assets, your organisation will become a moving target for cybercriminals.
WHY CHECK POINT AND BT

Check Point and BT form one of the strongest partnerships in cyber security. The combination of BT’s reach and Check Point’s innovative technologies and support services provide the highest levels of security in over 100 countries. BT has expert security engineers, as well as experience in deploying and managing complex environments using Check Point security solutions across the globe. BT already manages over 6,000 Check Point security gateways on behalf of customers all over the world including Fortune and Global 100 companies. That’s why BT is accredited to deliver Check Point products and services into a global market. In April 2016, Check Point named BT as ‘Systems Integrator Partner of the Year’.

Those of us on the front lines of enterprise security see the reality of modern hacking techniques, where anti-virus solutions are becoming less dependable against these newer threats. It is critical not only to do the best job possible detecting the latest malware, but also to respond rapidly as events occur. By preventing more attacks from reaching our users, and then empowering our team to quickly contain threats before they can impact operations, we allow our highly mobile workforce to manage their business with confidence.

Michael Brine, Infrastructure Manager, Community Newspaper Group
ABOUT THE AUTHORS

Aatish Pattni – Head of Threat Prevention, Northern Europe, Check Point Software Technologies

Aatish is responsible for the regional go-to-market strategy, channel enablement and direction for Check Point’s award winning SandBlast technology portfolio. As a recognized industry speaker he regularly delivers talks at InfoSec, IP Expo, The European Information Security Summit, NISC UK and several Business Reporter events.

Prior to joining Check Point, Aatish was Commercial Director at Bytes Security Partnerships where he lead business growth, client relationships and vendor strategy over a 10 years period. Over his career in the UK security industry Aatish has worked with some of the largest customers, resellers and vendors. During this time he has built a unique understanding of the challenges faced by clients around perimeter defense, threat prevention, data loss and the growing impact of cybercrime on business. Aatish holds a BSc in Computer Science, Software Engineering and Business Studies from Birmingham University, England.


Since joining BT ten years ago Luke has had a number of roles all with a focus on Service Delivery and more recently Security Service Delivery. Previously General Manager of BTs Cyber Defence Operations Luke spent two years in this role building and running a team of Security experts to counter the ever increasing cyber security threat. Before this Luke was General Manager of BTs Metal Theft Task Force responsible for all BTs activities to minimise the impact of cable theft on its customers. As well as driving a number of internal initiatives to minimise the service impact of cable theft he also worked externally with Industry partners, Law Enforcement Agencies and Government to help increase the level of collaborative working to tackle the problem ultimately resulting in changes to legislation.

As Vice President, Security UK and Global Banking and Financial Markets Luke is now working to take BTs continually evolving security capability to market.
To find out more about how working with BT and Check Point can help your business benefit from integrating smart prevention with detection and response, contact us on 0207 628 4211 or email uk_marketing@checkpoint.com